I

(Rezolucje, zalecenia i opinie)

OPINIE

EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Opinia Europejskiego Inspektora Ochrony Danych w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady zmieniającej dyrektywy 89/666/EWG, 2005/56/WE i 2009/101/WE w zakresie integracji rejestrów centralnych, rejestrów handlowych i rejestrów spółek

(2011/C 220/01)

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 wniosek o wydanie opinii zgodnie z art. 28 ust. 2 rozporządzenia (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],

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

I. WPROWADZENIE

1. W dniu 24 lutego 2011 r. Komisja Europejska przyjęła wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady zmieniającej dyrektywy 89/666/EWG, 2005/56/WE i 2009/101/WE w zakresie integracji rejestrów centralnych, rejestrów handlowych i rejestrów spółek [3] (zwany dalej „wnioskiem"), a następnie skonsultowała się z EIOD.

2. EIOD przyjmuje z zadowoleniem tę konsultację, której wymaga art. 28 ust. 2 rozporządzenia (WE) nr 45/2001, a także fakt, że odniesienie do niniejszej opinii znalazło się w preambule wniosku.

1.1. Cele wniosku

3. Celem wniosku jest ułatwienie i zwiększenie transgranicznej współpracy i wymiany informacji pomiędzy rejestrami przedsiębiorstw w Europejskim Obszarze Gospodarczym, a przez to zwiększenie przejrzystości i wiarygodności informacji dostępnych na poziomie transgranicznym. Sprawne procedury współpracy administracyjnej w zakresie rejestrów przedsiębiorstw mają zasadnicze znaczenie dla zwiększenia zaufania do europejskiego jednolitego rynku, poprzez zapewnienie bezpieczniejszego środowiska gospodarczego dla konsumentów, wierzycieli i innych partnerów biznesowych, zmniejszenie obciążeń administracyjnych i zwiększenie pewności prawa. Poprawa procedur współpracy administracyjnej w zakresie rejestrów przedsiębiorstw w Europie ma szczególne znaczenie dla transgranicznego łączenia spółek, przenoszenia siedziby i aktualizacji rejestracji zagranicznych oddziałów w przypadku braku mechanizmów współpracy lub ich ograniczonego zakresu.

4. W tym celu wniosek ma zmienić trzy istniejące dyrektywy w następujący sposób:

[1] Dz.U. L 281 z 23.11.1995, s. 31.
[2] Dz.U. L 8 z 12.1.2001, s. 1.
[3] Dla zwięzłości „rejestry centralne, rejestry handlowe i rejestry spółek" będą określane w dalszej części niniejszej opinii jako „rejestry przedsiębiorstw".

— celem zmian dyrektywy 2009/101/WE ([1]) jest ułatwienie transgranicznego dostępu do oficjalnych informacji o przedsiębiorstwach poprzez (i) utworzenie elektronicznej sieci rejestrów przedsiębiorstw; i (ii) określenie wspólnego minimalnego zestawu aktualnych informacji, które miałyby być udostępniane osobom trzecim za pomocą środków elektronicznych, za pośrednictwem wspólnej europejskiej wielojęzycznej platformy/punktu dostępu,

— zmiany dyrektywy 89/666/EWG ([2]) mają zapewnić przekazywanie przez rejestr aktualnych informacji o statusie spółki do rejestrów zagranicznych oddziałów w całej Europie,

— celem zmian dyrektywy 2005/56/WE ([3]) jest usprawnienie procedur współpracy administracyjnej pomiędzy rejestrami przedsiębiorstw w zakresie procedur dotyczących transgranicznego łączenia się spółek.

1.2. **Kontekst wniosku**

5. Rejestry przedsiębiorstw istnieją w każdym państwie członkowskim; są zorganizowane na poziomie krajowym, regionalnym lub lokalnym. W 1968 r. przyjęto wspólne zasady w celu ustanowienia minimalnych norm w zakresie ujawniania (rejestracji i publikacji) informacji o przedsiębiorstwach ([4]). Od dnia 1 stycznia 2007 r. państwa członkowskie muszą prowadzić elektroniczne rejestry przedsiębiorstw ([5]) i udostępniać stronom trzecim treść rejestru on-line.

6. Współpracy w zakresie rejestrów przedsiębiorstw z poszczególnych państw członkowskich wymagają wprost niektóre europejskie instrumenty prawne w celu ułatwienia transgranicznych połączeń spółek kapitałowych ([6]), przeniesienia siedziby spółki europejskiej (SE) ([7]) i spółdzielni europejskiej (SCE) ([8]).

7. W 1992 r. utworzono dobrowolny mechanizm współpracy w zakresie rejestrów przedsiębiorstw w Europie. Obecnie europejski rejestr przedsiębiorstw („EBR") ([9]) łączy oficjalne rejestry przedsiębiorstw z 19 państw członkowskich i sześciu innych europejskich systemów prawnych. W latach 2006–2009 EBR uczestniczył w projekcie badawczym BRITE ([10]), którego celem było stworzenie technicznej platformy dla interoperacyjności rejestrów przedsiębiorstw w całej Europie. Ocena skutków dołączona do wniosku wyjaśnia jednak, że EBR napotyka poważne trudności w zakresie rozbudowy, finansów i zarządzania: zgodnie z oceną skutków dzisiejszy mechanizm współpracy, w obecnej formie, nie jest w pełni zadowalający dla potencjalnych użytkowników.

1.3. **Synergie z innymi inicjatywami**

8. W uzasadnieniu dołączonym do wniosku zauważono, że europejski portal e-sprawiedliwość ([11]) ma się stać centralnym punktem dostępu do informacji prawnych, instytucji prawnych i administracyjnych, rejestrów, baz danych i innych usług w UE. Ponadto potwierdzono, że wniosek stanowi uzupełnienie projektu e-sprawiedliwość i powinien przyczynić się do łatwiejszego dostępu do informacji o przedsiębiorstwach dla stron trzecich za pośrednictwem tego portalu.

9. Zgodnie z oceną skutków innym ważnym projektem o potencjalnych synergiach jest system wymiany informacji na rynku wewnętrznym (IMI) ([12]). IMI to elektroniczne narzędzie mające wspierać codzienną współpracę administracyjną pomiędzy publicznymi systemami administracji w kontekście dyrektywy w sprawie usług (2006/123/WE) i dyrektywy w sprawie kwalifikacji zawodowych (2005/36/WE). IMI jest obecnie na etapie rozbudowy i mógłby, zgodnie z oceną skutków, wesprzeć również wdrażanie innych dyrektyw, w tym dyrektyw w dziedzinie prawa spółek.

II. **WŁAŚCIWE PRZEPISY WNIOSKU**

10. Artykuł 3 wniosku zmienia dyrektywę 2009/101/WE pod kilkami względami. Spośród tych zmian dwie są bardzo istotne dla ochrony danych.

([1]) Dyrektywa 2009/101/WE Parlamentu Europejskiego i Rady z dnia 16 września 2009 r. w sprawie koordynacji gwarancji, jakie są wymagane w państwach członkowskich od spółek w rozumieniu art. 48 akapit drugi Traktatu, w celu uzyskania ich równoważności, dla zapewnienia ochrony interesów zarówno wspólników, jak i osób trzecich (Dz.U. L 258 z 1.10.2009, s. 11).

([2]) Jedenasta dyrektywa Rady z dnia 21 grudnia 1989 r. dotycząca wymogów ujawniania informacji odnośnie do oddziałów utworzonych w państwie członkowskim przez niektóre rodzaje spółek podlegające prawu innego państwa (Dz.U. L 395 z 30.12.1989, s. 36).

([3]) Dyrektywa 2005/56/WE Parlamentu Europejskiego i Rady z dnia 26 października 2005 r. w sprawie transgranicznego łączenia się spółek kapitałowych (Dz.U. L 310 z 25.11.2005, s. 1).

([4]) Przytoczona powyżej w całości dyrektywa 2009/101/WE. Artykuł 1 dyrektywy ogranicza zakres przepisów dyrektywy do „spółek kapitałowych".

([5]) Dyrektywa 2003/58/WE Parlamentu Europejskiego i Rady z dnia 15 lipca 2003 r. zmieniająca dyrektywę Rady 68/151/EWG w zakresie wymagań dotyczących jawności w odniesieniu do niektórych typów spółek (Dz.U. L 221 z 4.9.2003, s. 13).

([6]) Przytoczona powyżej w całości dyrektywa 2005/56/WE.

([7]) Rozporządzenie Rady (WE) nr 2157/2001 z dnia 8 października 2001 r. w sprawie statutu spółki europejskiej (SE) (Dz.U. L 294 z 10.11.2001, s. 1).

([8]) Rozporządzenie Rady (WE) nr 1435/2003 z dnia 18 sierpnia 2003 r. w sprawie statutu spółdzielni europejskiej (SCE) (Dz.U. L 207 z 18.8.2003, s. 1).

([9]) http://www.ebr.org/

([10]) http://www.briteproject.eu

([11]) https://e-justice.europa.eu/home.do

([12]) http://ec.europa.eu/internal_market/imi-net/index_en.html

2.1. **Publikacja informacji za pośrednictwem europejskiej elektronicznej platformy/punktu dostępu**

11. Obowiązujący obecnie art. 2 dyrektywy 2009/101/WE wymaga już, by pewne minimalne informacje były ujawniane w rejestrze przedsiębiorstw każdego państwa członkowskiego, przez co strony trzecie są w stanie ustalić informacje o spółkach. Jak wyjaśniono w pkt 1.2 powyżej, państwa członkowskie muszą również prowadzić elektroniczne rejestry przedsiębiorstw i udostępniać stronom trzecim treść tych rejestrów on-line.

12. Artykuł 2 wymienia jedenaście podstawowych informacji o spółce, które należy udostępnić publicznie, między innymi:

— akt założycielski, status i ewentualne zmiany tych dokumentów,

— kapitał subskrybowany,

— dokumenty księgowe,

— zmiana siedziby spółki,

— likwidacja, stwierdzenie nieważności umowy spółki; powołanie likwidatorów, zakończenie postępowania likwidacyjnego, wykreślenie z rejestru.

13. Co ważne z punktu widzenia ochrony danych, art. 2 wymaga również ujawnienia „powołania, zakończenia sprawowania funkcji, jak też danych" (podkreślenia własne) osób, które są (i) upoważnione do reprezentowania spółki; lub (ii) w innymi zakresie uczestniczą w „zarządzaniu, nadzorowaniu lub kontrolowaniu" spółki.

14. Lista informacji do ujawnienia wymaganych zgodnie z art. 2 nie uległa zmianie we wniosku. Wymóg publicznego udostępnienia tych informacji przez każde państwo członkowskie w formie elektronicznej także nie jest nowy. Nowością we wniosku jest to, że informacje dotychczas dostępne fragmentarycznie, często jedynie w lokalnych językach i poprzez lokalne strony internetowe, obecnie będą łatwo dostępne, poprzez wspólną europejską platformę/punkt dostępu, w wielojęzycznym środowisku.

15. W tym celu wniosek wprowadziłby nowy art. 3a do dyrektywy, który stanowi, że: „Państwa członkowskie dopilnowują, aby złożone w ich rejestrze dokumenty i informacje, o których mowa w art. 2, były na wniosek każdego wnioskodawcy dostępne drogą elektroniczną poprzez wspólną europejską platformę elektroniczną dostępną z terytorium każdego państwa członkowskiego". Wniosek odsyła w zakresie szczegółowych wymogów do aktów delegowanych.

2.2. **Interoperacyjność i integracja rejestrów przedsiębiorstw: ustanowienie sieci elektronicznej**

16. Wniosek wprowadziłby również nowy art. 4a do tej samej dyrektywy 2009/101/WE, który stanowi, że: „Państwa członkowskie podejmują niezbędne działania w celu dopilnowania, aby [rejestry przedsiębiorstw] były interoperacyjne i tworzyły sieć elektroniczną". Wniosek ponownie odsyła w zakresie szczegółowych wymogów do aktów delegowanych.

2.3. **Przepisy dotyczące ochrony danych**

17. W celu objęcia kwestii ochrony danych wniosek wprowadziłby również do tekstu wszystkich trzech zmienianych dyrektyw odrębny artykuł o ochronie danych, stanowiący, że „[p]rzetwarzanie danych osobowych, które odbywa się w kontekście [dyrektywy], podlega przepisom dyrektywy 95/46/WE".

III. **UWAGI I ZALECENIE EIOD**

3.1. **Wprowadzenie: spełnienie wymogów w zakresie przejrzystości i prywatności**

18. EIDO podziela opinię Komisji, że (i) zastosowanie technologii informacyjno-komunikacyjnych może pomóc zwiększyć wydajność współpracy w zakresie rejestrów przedsiębiorstw; oraz (ii) zwiększenie dostępności informacji z rejestrów przedsiębiorstw może prowadzić do większej przejrzystości. Stąd popiera cele wniosku. Jego uwagi należy ocenić w świetle tego konstruktywnego podejścia.

19. Jednocześnie EIOD podkreśla także, że większa dostępność danych osobowych również prowadzi do większych zagrożeń dla danych osobowych. Dla przykładu, o ile prawidłowa identyfikacja przedstawiciela spółki może być łatwiejsza, jeśli jego prywatny adres jest ujawniony, ujawnienie to mogłoby mieć również negatywny wpływ na prawo tej osoby fizycznej do ochrony danych osobowych. Jest tak w szczególności w przypadku danych osobowych szeroko udostępnianych w Internecie w formie cyfrowej, w wielu językach, poprzez łatwo dostępną europejską platformę/punkt dostępu.

20. Jeszcze nie tak dawno dane osobowe z rejestrów przedsiębiorstw (np. imię i nazwisko, adres i wzór podpisu dyrektora) były często udostępniane publicznie w formie papierowej i w lokalnym języku, wymagając jedynie osobistej wizyty wnioskodawcy w lokalnym urzędzie rejestracyjnym. Należy uznać, że sytuacja ta jest jakościowo inna od publicznego udostępniania danych w formie cyfrowej,

za pośrednictwem ogólnokrajowego elektronicznego punktu dostępu. Publiczne ujawnianie danych osobowych za pośrednictwem łatwo dostępnej ogólnoeuropejskiej platformy/punktu dostępu jest kolejnym krokiem naprzód i jeszcze bardziej zwiększa dostępność informacji oraz zagrożenia dla ochrony danych osobowych osób, których dane dotyczą.

21. Wśród zagrożeń dla prywatności (z powodu łatwego dostępu do danych w formie cyfrowej, za pośrednictwem elektronicznego punktu dostępu) jest kradzież tożsamości i inne działania przestępcze oraz ryzyko, że ujawniane informacje będą niezgodnie z prawem gromadzone i wykorzystywane przez spółki do celów handlowych, pierwotnie nieprzewidzianych, w wyniku profilowania osób, których dane dotyczą. Bez odpowiednich gwarancji informacje mogą być także sprzedawane innym lub łączone z innym informacjami i odsprzedawane rządom do wykorzystania do niepowiązanych i nieujawnionych celów (na przykład wdrażania prawa podatkowego lub innych karnych lub administracyjnych dochodzeń) bez odpowiedniej podstawy prawnej ([1]).

22. Z tych względów należy starannie ocenić, czy dane osobowe powinny być udostępniane za pośrednictwem wspólnej europejskiej platformy/punktu dostępu i jakie dodatkowe gwarancje ochrony danych – w tym techniczne środki ograniczające możliwości wyszukiwania lub pobierania danych oraz eksplorację danych – powinny znaleźć zastosowanie.

3.2. **Istotne gwarancje ochrony danych należy określić w samym wniosku, a nie w aktach delegowanych**

23. Jak zauważono w pkt 2.1 i 2.2 powyżej, zaproponowane art. 3a i 4a dyrektywy 2009/101/WE są bardzo ogólne i pozostawiają wiele kluczowych kwestii aktom delegowanym.

24. Choć EIOD uznaje potrzebę elastyczności, a tym samym także konieczność aktów delegowanych, podkreśla, że niezbędne gwarancje ochrony danych są istotnymi elementami, które powinny mieć wyraźne i odrębne miejsce bezpośrednio w samym tekście wniosku dotyczącym dyrektywy. W tym względzie nie można ich postrzegać jako „elementów innych niż istotne", które można zamieścić w kolejnych aktach delegowanych przyjmowanych zgodnie z art. 290 Traktatu o funkcjonowaniu Unii Europejskiej.

25. Stąd EIOD zaleca, by przepisy wniosku dotyczące ochrony danych były bardziej szczegółowe i nie były tylko zwykłym odniesieniem do dyrektywy 95/46/WE (zobacz pkt 3.4–3.13). Dodatkowe przepisy odnoszące się do wdrażania szczegółowych gwarancji można następnie zamieścić w aktach delegowanych, po konsultacji z EIOD oraz w stosownych przypadkach – z krajowymi organami ochrony danych (zobacz pkt 3.5, 3.6, 3.8, 3.9, 3.10, 3.12 i 3.13 poniżej).

3.3. **Inne istotne elementy zaproponowanych środków należy również wyjaśnić w samym wniosku**

26. Wniosek nie milczy tylko na temat kluczowych gwarancji ochrony danych, jest także otwarty w innych względach. W szczególności pozostawia aktom delegowanym określenie istotnych elementów w zakresie tego, jak zamierza zapewnić zaproponowaną (i) integrację rejestrów przedsiębiorstw; i (ii) publiczne ujawnianie danych.

27. Jasność tych pozostałych istotnych elementów wniosku jest warunkiem wstępnym przyjęcia odpowiednich gwarancji ochrony danych. Stąd EIOD zaleca, by te istotne elementy zostały określone w samym wniosku dotyczącym dyrektywy (zobacz pkt 3.4 i 3.5 poniżej).

3.4. **Zarządzanie: należy wyjaśnić we wniosku dotyczącym dyrektywy role, kompetencje i obowiązki**

28. Obecnie wniosek pozostawia aktom delegowanym określenie zasad w zakresie zarządzania siecią elektroniczną, jej administracji oraz funkcjonowania i reprezentowania ([2]).

29. O ile ocena skutków i uzasadnienie określają pewne synergie z IMI i portalem e-sprawiedliwość, tekst wniosku dotyczącego dyrektyw pozostawia otwarte różne opcje urzeczywistnienia się pewnej lub wszystkich synergii, w tym przeprojektowanie EBR, wykorzystanie IMI do wymiany określonych danych lub wykorzystanie portalu e-sprawiedliwości jako platformy/punktu dostępu do dostarczania społeczeństwu informacji z rejestrów przedsiębiorstw.

30. Nie wykluczono również innych opcji, takich jak ogłoszenie przetargu na przyznanie prawa do zaprojektowania i prowadzenia sieci elektronicznej lub Komisja podejmująca się bezpośredniej roli w projektowaniu i prowadzeniu systemu. Przedstawiciele państwa członkowskiego mogą również być częścią struktury zarządczej sieci elektronicznej.

([1]) Rośnie rynek, na którym sprzedawane są tego typu informacje o przedsiębiorstwach: usługodawcy na tym rynku zdobywają wiarygodność u spółek/osób fizycznych w oparciu o informacje zgromadzone z wielu miejsc, w tym rejestrów przedsiębiorstw, rejestrów sądowych, rejestrów postępowań upadłościowych itp.

([2]) Zob. zaproponowane brzmienie art. 4a ust. 3 lit. a) dyrektywy 2009/101/WE.

31. Ponadto, choć wniosek, w obecnej formie, przewiduje „wspólną europejską platformę elektroniczną" (podkreślenia własne), nie sposób wykluczyć, że tekst zostanie zmieniony na późniejszym etapie procedury ustawodawczej w celu zapewnienia bardziej zdecentralizowanej struktury.

32. EIOD zauważa również, że choć obecny wniosek nie zajmuje się odrębnie kwestią integracji rejestrów przedsiębiorstw z innymi bazami danych (takimi jak rejestry gruntów lub rejestry stanu cywilnego), istnieje z pewnością taka możliwość techniczna i proces ten zachodzi już w niektórych państwach członkowskich ([1]).

33. Wybór jednej lub drugiej z tych opcji może prowadzić do całkowicie innej struktury zarządzania siecią elektroniczną i narzędziem elektronicznym wykorzystywanym do publicznego udostępniania. To z kolei prowadzi do różnych ról i obowiązków zaangażowanych stron, a tym samym innych ról i obowiązków z punktu widzenia ochrony danych.

34. W tym względzie EIOD podkreśla, że w każdym przypadku przetwarzania danych osobowych ważne jest prawidłowe określenie, kto jest „administratorem danych". Podkreśla to również Grupa Robocza Art. 29 ds. Ochrony Danych Osobowych w swojej opinii 1/2010 dotyczącej pojęć „administrator danych" i „podmiot przetwarzający" ([2]). Podstawowym powodem, dlaczego jasna i jednoznaczna identyfikacja administratora danych jest tak ważna jest fakt, że określona ona, kto jest odpowiedzialny za zgodność z zasadami ochrony danych. Ma ona także znaczenie przy określaniu właściwych przepisów ([3]).

35. Jak zauważono w opinii Grupy Roboczej Art. 29, „jeśli nie jest dostatecznie jasne, od kogo się czego wymaga – np. nikt nie jest odpowiedzialny lub jest wielu potencjalnych administratorów danych – istnieje oczywiste ryzyko, że niewiele się wydarzy, jeśli w ogóle, i że przepisy pozostaną nieskuteczne".

36. EIOD podkreśla, że jasność jest szczególnie potrzebna w sytuacjach, gdy wiele podmiotów uczestniczy w relacji współpracy. Jest tak często w przypadku systemów informacji UE wykorzystywanych do celów publicznych, gdy cel przetwarzania danych jest zdefiniowanych w prawie UE.

37. Z tych względów EIOD zaleca ustalenie, w tekście samego wniosku dotyczącego dyrektywy, w odrębny, jasny i jednoznaczny sposób:

— czy sieć elektroniczna będzie prowadzona przez Komisję, czy przez stronę trzecią oraz czy będzie miała scentralizowaną, czy zdecentralizowaną strukturę,

— zadań i obowiązków każdej strony zaangażowanej w przetwarzanie danych i zarządzanie siecią elektroniczną, w tym Komisji, przedstawicieli państw członkowskich, posiadaczy rejestrów przedsiębiorstw w państwach członkowskich i stron trzecich,

— związku pomiędzy systemem elektronicznym przewidzianym we wniosku a innymi inicjatywami, takimi jak IMI portal e-sprawiedliwości i EBR.

38. Z perspektywy ochrony danych te wyjaśnienia powinny być także szczegółowe i jednoznaczne w celu ustalenia, na podstawie samego wniosku dotyczącego dyrektywy, czy dany podmiot należy postrzegać jako „administratora danych" lub „podmiot przetwarzający".

39. Zasadniczo wniosek powinien wyraźnie przyczyniać się do ustalenia, jak wydaje się wynikać z obecnego wniosku w całości, że posiadaczy rejestrów przedsiębiorstw, jak i operatora(-ów) systemu należy postrzegać bez wyjątku jako administratorów danych w zakresie ich działalności. W związku z tym, uznając, że obecnie wniosek nie opisuje struktury zarządzania i nie określa operatora(-ów) systemu elektronicznego, nie można wykluczyć, że określony podmiot lub określone podmioty, które będą ostatecznie prowadzić system w praktyce, będą funkcjonować jako podmioty przetwarzające, a nie jako „administratorzy danych". Może tak się stać w szczególności, jeśli działalność ta jest zlecana na zewnętrz stronie trzeciej, która będzie ściśle stosować się do poleceń. W każdym razie wydaje się, że pozostaje wiele administratorów danych, co najmniej jeden w każdym państwie członkowskim: podmioty, które prowadzą rejestry przedsiębiorstw. Fakt, że mogą istnieć inne (prywatne) podmioty zaangażowane jako operatorzy, „dystrybutorzy" lub w inny sposób, nie zmienia tej kwestii. W każdy razie należy zamieścić to we wniosku dotyczącym dyrektywy w celu zapewnienia jasności i pewności prawa.

([1]) Uznając, że integracja nie jest obecnie przewidziana we wniosku, EIOD nie będzie omawiał tej kwestii w swojej opinii na tym etapie. Zwraca jednak uwagę, że jeśli integrację należałoby uwzględnić, mogłoby to wymagać oddzielnej analizy proporcjonalności i przyjęcia dodatkowych odpowiednich gwarancji ochrony danych.

([2]) Zob. art. 2 lit. d) i e) dyrektywy 95/46 i rozporządzenia (WE) nr 45/2001; także opinia 1/2010 z dnia 16 lutego 2010 Grupy Roboczej Art. 29 ds. Ochrony Danych dotycząca pojęcia „administrator danych" i „podmiot przetwarzający" (WP169).

([3]) Biorąc pod uwagę, że przepisy dotyczące ochrony danych nie są w pełni ujednolicone w całej Europie, tożsamość administratora danych jest istotna dla ustalenia, które krajowe przepisy mają zastosowanie. Ponadto należy także ustalić, czy dyrektywa 95/46 lub rozporządzenie (WE) nr 45/2001 ma zastosowanie: jeśli Komisja jest (także) administratorem danych, rozporządzenie (WE) nr 45/2001 będzie miało (także) zastosowanie, jak wyjaśniono w pkt 3.11 poniżej.

40. W końcu wniosek powinien również opisać bardziej szczegółowo i pełnie obowiązki, które wynikają z tych ról. Na przykład rola operatora(-ów) w dopilnowaniu, by system został zaprojektowany z poszanowaniem prywatności oraz jego rola koordynująca w odniesieniu do kwestii ochrony danych powinny znaleźć się we wniosku.

41. EIOD zauważa, że wszystkie te wyjaśnienia będą również istotne przy ustalaniu, które organy nadzoru ochrony danych są właściwe i dla którego przetwarzania danych.

3.5. **Ramy i podstawa prawna przepływów danych/procedur współpracy administracyjnej powinny być zdefiniowane we wniosku dotyczącym dyrektywy**

42. Wydaje się, że nie przewidziano, by sieć elektroniczna, w jej obecnej formie, automatycznie udostępniała wszystkie informacje przechowywane w każdym rejestrze przedsiębiorstw wszystkim innym rejestrom przedsiębiorstw we wszystkich innych państwach członkowskich: wniosek wymaga jedynie integracji i interoperacyjności rejestrów przedsiębiorstw, a tym samym wprowadza warunki pozwalające na wymianę informacji i dostęp do nich w przyszłości. W celu zapewnienia pewności prawa wniosek powinien wyjaśniać, czy to rozumowanie jest prawidłowe.

43. Ponadto wniosek nie określa również, jakie przepływy danych/procedury współpracy administracyjnej mogą mieć miejsce poprzez zintegrowane rejestry przedsiębiorstw ([1]). EIOD rozumie, że pewna elastyczność może być konieczna w celu zapewnienia możliwości spełnienia potrzeb, które pojawią się w przyszłości. Mimo to EIOD uważa za niezbędne określenie we wniosku ram dla tych przepływów danych i procedury współpracy administracyjnej, które mogą mieć miejsce w przyszłości za pośrednictwem sieci elektronicznej. Jest to szczególnie istotne w celu dopilnowania, by (i) wymiana danych odbywała się na solidnej podstawie prawnej; i by (ii) zostały zapewnione odpowiednie gwarancje ochrony danych.

44. Według EIOD wymiana danych lub inne przetwarzanie danych przy użyciu sieci elektronicznej (np. publiczne udostępnianie danych osobowych za pośrednictwem wspólnej platformy/punktu dostępu) powinny być oparte na wiążącym akcie UE przyjętym na solidnej podstawie prawnej. Powinno to zostać wyraźnie określone we wniosku dotyczącym dyrektywy ([2]).

([1]) Jest tak z wyjątkiem, w pewnym zakresie, wymiany danych w przypadku transgranicznego łączenia się spółek, przenoszenia siedziby i aktualizacji informacji o oddziałach, które szczegółowo omówiono we wniosku.

([2]) W tym względzie, jeśli jest potencjalna konieczność przetwarzania danych na obszarze rynku wewnętrznego, który nie jest objęty odrębnym aktem Unii, EIOD wzywa do dalszej analizy szczegółowych zasad dla ram prawnych, co mogłoby pozwolić, być może w powiązaniu z ogólnymi przepisami Traktatu, na szczegółowe przepisy we wniosku dotyczącym dyrektywy, i kolejnych aktach delegowanych, w celu zapewnienia odpowiedniej podstawy prawnej z punktu widzenia ochrony danych. We wniosku dotyczącym dyrektywy należy również określić, czy rejestry przedsiębiorstw mogą wykorzystywać sieć elektroniczną i wspólny punkt dostępu do wymiany lub publicznego udostępniania danych osobowych nieprzewidzianej w akcie Unii, ale dozwolonej lub wymaganej zgodnie z przepisami krajowymi.

3.6. **Inne kluczowe kwestie pozostawione dla aktów delegowanych powinny również zostać omówione we wniosku dotyczącym dyrektywy**

45. Ponadto wniosek stanowi, że akty delegowane określają następujące kwestie ([3]):

— warunki uczestniczenia w sieci elektronicznej dla państw poza Europejskim Obszarem Gospodarczym,

— minimalne normy bezpieczeństwa dla sieci elektronicznej, oraz,

— definicję norm w zakresie formatu, treści i ograniczeń dla przechowywania i wyszukiwania dokumentów i informacji, umożliwiających automatyczną wymianę danych.

46. W zakresie pierwszego i drugiego tiret EIOD zauważa, że niektóre istotne gwarancje powinny zostać ustanowione w samym wniosku dotyczącym dyrektywy (zobacz pkt 3.12 i 3.13 poniżej). Więcej szczegółowych informacji można następnie zawrzeć w aktach delegowanych.

47. W zakresie automatycznej wymiany danych EIOD z zadowoleniem zauważa, że wniosek wymaga od aktów delegowanych wprowadzenie „definicji norm w zakresie formatu, treści i ograniczeń dla przechowywania i wyszukiwania dokumentów i informacji, umożliwiających automatyczną wymianę danych".

48. Aby uzyskać większą jasność w tym względzie EIOD zaleca, by sam wniosek dotyczący dyrektyw wyraźnie określał, że elektroniczna sieć umożliwia (i) odrębną, ręczną, indywidualną wymianę danych pomiędzy rejestrami przedsiębiorstw (zgodnie z aktem UE, jak w przypadku łączenia spółek lub przenoszenia siedziby); oraz (ii) automatyczne przekazywanie danych (zgodnie z aktem UE, jak w przypadku aktualizacji informacji w rejestrze zagranicznych oddziałów).

([3]) Zob. zaproponowane brzmienie art. 4a ust. 3 dyrektywy 2009/101/WE.

49. W celu osiągnięcia jeszcze większej jasności EIOD zaleca również, by tekst wniosku dla odnośnego art. 4a ust. 3 lit. i) dyrektywy 2009/101/WE został zmieniony w sposób gwarantujący, że (i) akty delegowane będą w pełni obejmować ręczną i automatyczną wymianę danych; (ii) są objęte wszystkie operacje przetwarzania danych, które mogą dotyczyć danych osobowych (nie tylko przechowywanie i wyszukiwanie); oraz że (iii) odrębne przepisy dotyczące ochrony danych w aktach delegowanych będą również zapewniać praktyczne stosowanie istotnych gwarancji ochrony danych.

50. Przykładowo art. 4a ust. 3 lit. i) mógłby otrzymać brzmienie:

„i) format, treść i ograniczenia dla operacji ręcznego lub automatycznego przetwarzania danych odbywających się przy użyci sieci, w tym przekazywania, przechowywania i wyszukiwania informacji; oraz odrębne środki, które mogą być konieczne dla zapewnienia praktycznego stosowania istotnych gwarancji ochrony danych".

3.7. **Kategorie przetwarzanych danych osobowych powinny także zostać wyjaśnione we wniosku dotyczącym dyrektywy**

51. Na wstępie EIOD podkreśla, że imiona i nazwiska (i ewentualnie inne dane, takie jak prywatne adresy) przedstawicieli spółek (i innych osób fizycznych zaangażowanych w zarządzanie spółkami) bez wątpienia stanowią najbardziej oczywiste dane osobowe, które mogą być przetwarzane przy użyciu sieci elektronicznej lub udostępniane publicznie za pomocą wspólnej platformy elektronicznej/punktu dostępu, nie są to jednak w żadnym razie jedyne dane osobowe przechowywane w rejestrach przedsiębiorców.

52. Po pierwsze, niektóre dokumenty wymienione w art. 2 dyrektywy 2009/101/WE (np. akt założycieli, status i dokumenty księgowe) mogą również zawierać dane osobowe innych osób fizycznych. Dane mogą obejmować między innymi imiona i nazwiska, adresy, ewentualnie numery identyfikacyjne i daty urodzenia, a nawet skany podpisów ręcznych różnych osób fizycznych, w tym osób, które założyły spółkę, udziałowców spółki, prawników, księgowych, pracowników lub notariuszy publicznych.

53. Po drugie, dane spółki, połączone z imieniem i nazwiskiem osoby fizycznej (takiej jak dyrektor) można również uznać za dane osobowe odnoszące się do tej osoby. Na przykład, jeśli dane z rejestru przedsiębiorstw pokazują, że dana osoba jest w zarządzie spółki w trakcie likwidacji, informacja ta jest również istotna dla tej osoby.

54. W celu zapewnienia jasności, jakie dane osobowe są przetwarzane oraz dopilnowania, by zakres przetwarzanych danych był proporcjonalny do celów wniosku, EIOD zaleca poniższe wyjaśnienia określone w pkt 3.7.

Sformułowanie „dane osób" (particulars of persons) należy wyjaśnić we wniosku dotyczącym dyrektywy

55. Artykuł 2 dyrektywy 2009/101/WE nie określa, które „dane" odnośnych osób (przedstawicieli spółki i innych osób zaangażowanych w zarządzanie spółką) należy ujawnić.

56. Różne wersje językowe wniosku wykazują natomiast różnice nawet w odniesieniu do przekładu sformułowania „dane osób". Na przykład sformułowanie otrzymało brzmienie „l'identité des personnes" (tj. tożsamość osób) w języku francuskim, „le generalità delle persone" (tj. dane osobiste, takie jak imię i nazwisko) w języku włoskim, „személyek adatai" (tj. dane osób) w języku węgierskim, „de identiteit van de personen" (tj. tożsamość osób) w języku niderlandzkim i „identitatea persoanelor" (tj. tożsamość osób) w języku rumuńskim.

57. Ponadto, w niektórych państwach członkowskich prywatne adresy dyrektorów spółek lub innych osób, takich jak niektórzy udziałowcy, są standardowo upubliczniane w Internecie. W innych państwa członkowskich informacje te są przechowywane jako poufne w rejestrze przedsiębiorstw, do których składa się te informacje, ze względu na poufność, w obawie przed kradzieżą tożsamości.

58. EIOD zaleca wprowadzenie zmian do art. 2 dyrektywy 2009/101/WE w celu wyjaśnienia, które dane osobowe, jeśli którekolwiek, obok imion i nazwisk odnośnych osób (przedstawicieli spółki i innych osób zaangażowanych w zarządzanie spółką) należy ujawnić. Należy przy tym starannie uwzględnić konieczność przejrzystości i odpowiedniej identyfikacji tych osób, jednocześnie pamiętając o innych przeciwległych aspektach, takich jak konieczność ochrony prywatności odnośnych osób ([1]).

59. Jeśli nie dojdzie do porozumienia z powodu różnic w krajowych praktykach, art. 2 powinien zostać zmieniony tak, by wymagał ujawnienia „pełnego imienia i nazwiska odnośnych osób, i jeśli tego wymaga odrębnie prawo krajowe – dodatkowe dane niezbędne do ich identyfikacji". Będzie wtedy jasne, że każde państwo członkowskie ma

([1]) Ocena proporcjonalności powinna zostać przeprowadzona, w szczególności z uwzględnieniem kryteriów ustanowionych przez Europejski Trybunał Sprawiedliwości w sprawie Schecke i Elfert (wyrok Trybunału w sprawach połączonych C-92/09 i C-93/09 z listopada 2010 r.; zob. w szczególności pkt 81, 65 i 86). W sprawie Schecke Trybunał podkreślił, że odstępstwa i ograniczenia w stosunku do ochrony danych osobowych muszą mieć zastosowanie wyłącznie tam, gdzie to bezwzględnie konieczne. Trybunał dalej stwierdził, że instytucje powinny przeanalizować różne metody publikacji w celu odnalezienia tej jednej, która byłaby spójna z celem publikacji, jednocześnie w jak najmniejszym stopniu wpływając na prawo osób, których dane dotyczą, do poszanowania życia prywatnego w ogólności i ochrony danych osobowych w szczególności.

zadecydować, w przepisach krajowych, które „dane" (*particulars*) obok imion i nazwisk należy ujawnić oraz że dodatkowe dane osobowe będzie należało ujawnić tylko wtedy, gdy jest to konieczne do identyfikacji odnośnych osób.

60. Ewentualnie, uznając, że art. 2 wymienia „minimalne dane", a nie ujednolicając treść rejestrów przedsiębiorstw w całej Europie, sformułowanie „dane osób" (*particulars of persons*) można by zwyczajnie zastąpić wyrażeniem „pełne imiona i nazwiska osób" (*full names of persons*). Także do państwa członkowskiego należałaby wtedy decyzja, które dodatkowe informacje, jeśli którekolwiek, chce ujawniać.

Sformułowanie „zarządzani[e], nadzorowani[e] lub kontrolowani[e]" należy wyjaśnić

61. Artykuł 2 dyrektywy 2009/101/WE również wymaga ujawnienia informacji o osobach zaangażowanych w „zarządzani[e spółką], nadzorowani[e jej] lub kontrolowani[e]". To szerokie sformułowanie nie pozwala jasno stwierdzić, czy informacje odnoszące się do udziałowców należy ujawnić: w szczególności informacje o udziałowcach, którzy (i) mają znaczący, mający wpływ lub kontrolujący udział powyżej pewnego progu; lub (ii) na mocy złotych akcji, szczegółowych ustaleń umowny lub na innych zasadach mają skuteczną kontrolę nad przedsiębiorstwem lub wpływ na nie.

62. EIOD rozumie, że szerokie sformowanie jest wymagane w celu objęcia szeregu struktur zarządzania spółką, które obecnie istnieją dla spółek kapitałowych w poszczególnych państwach członkowskich. Mimo to pewność prawa w zakresie kategorii osób, których dane mogą zostać ujawnione, jest istotna z punktu widzenia ochrony danych. Stąd EIOD zaleca zmienić art. 2 dyrektywy 2009/101/WE w celu wyjaśnienia, jakie dane osobowe odnoszące się do udziałowców, jeśli któregokolwiek, należy ujawnić. Przy tym analiza proporcjonalności zgodnie z analizą w sprawie *Schecke* (jak zauważono powyżej) musi również zostać przeprowadzona.

Ujawnianie informacji powyżej wymaganego minimum; czarne listy

63. Choć wniosek nie wymaga wymiany lub publicznego ujawniania danych osobowych powyżej minimalnych wymogów określonych w art. 2 dyrektywy 2009/101/WE, nie wyklucza również, że państwa członkowskie, jeśli się na to zdecydują, mogły wymagać, by rejestry przedsiębiorstw przetwarzały lub ujawniały dalej dane osobowe oraz udostępniały takie dane także poprzez wspólną europejską platformę/punkt dostępu lub wymianę takich danych z rejestrami przedsiębiorstw w innych państwach członkowskich.

64. Jest to szczególnie delikatna kwestia w odniesieniu do „czarnych list". W niektórych krajach elektroniczny rejestr *de facto* funkcjonuje także jako rodzaj „czarnej listy" i może być przeszukiwany przez stronę trzecią przez portal elektroniczny dla informacji na temat przedstawicieli spółki, którym zakazano działalności.

65. Aby sprostać tej kwestii EIOD zaleca wyjaśnienie we wniosku, czy i w jakim zakresie państwa członkowskie mogą ostatecznie publicznie udostępnić więcej informacji poprzez wspólny portal lub mogą ostatecznie wymienić więcej informacji między sobą, w oparciu o ich własne krajowe przepisy, jeśli się na to zdecydują. W tym przypadku ścisła ocena proporcjonalności (zobacz przytoczona powyżej sprawa Schecke) powinna być oparta na przepisach krajowych, a także uwzględniać jako czynnik cele rynku wewnętrznego.

66. Ponadto EIOD sugeruje powiązanie wykorzystania tych uprawnień z rolą, jaką mają odegrać krajowe organy ochrony danych, na przykład, poprzez konsultację.

67. W końcu EIOD podkreśla, że gdyby europejski system miał z założenia wymagać takich „czarny list", powinno to zostać odrębnie określone we wniosku dotyczącym dyrektywy ([1]).

3.8. **Gwarancje mające na celu zapewnienie przestrzegania zasady celowości; zabezpieczenia przed gromadzeniem danych, eksploracją danych, łączeniem danych i niezgodnymi z przeznaczeniem wyszukaniami**

68. EIOD zaleca, by wniosek dotyczący dyrektywy szczegółowo określał, że we wszystkich przypadkach, w których dane osobowe są publicznie udostępniane albo są wymieniane pomiędzy rejestrami przedsiębiorstw, należy zapewnić odpowiednie zabezpieczenia, w szczególności przed gromadzeniem danych, eksploracją danych, łączeniem danych i niezgodnymi z przeznaczeniem wyszukaniami, w celu dopilnowania, by dane osobowe, które zostały udostępnione do celów przejrzystości nie zostały niewłaściwie wykorzystane do dodatkowych, niepowiązanych celów ([2]).

69. EIOD podkreśla w szczególności konieczność rozważenia technicznych i organizacyjnych środków, z uwzględnieniem zasady ochrony prywatności w fazie projektowania (zobacz pkt 3.14 poniżej). Praktyczne wdrożenie tych gwarancji można pozostawić do aktów delegowanych. Zasady powinny zostać jednak określone w samym wniosku dotyczącym dyrektywy.

([1]) Uznając, że obecnie kwestia ta nie jest przewidziana we wniosku, EIOD nie będzie jej omawiał bardziej szczegółowo w swojej opinii na tym etapie. Zwraca jednak uwagę, że jeśli kwestię tę należałoby uwzględnić, mogłoby to wymagać oddzielnej analizy proporcjonalności i przyjęcia dodatkowych odpowiednich gwarancji ochrony danych.

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

3.9. **Informacje dla osób, których dane dotyczą i przejrzystość**

70. EIOD zaleca, by wniosek dotyczący dyrektywy zawiera odrębny przepis wymagający, by informacje zgodnie z art. 10 i 11 dyrektywy 95/46/WE (a w stosownych przypadkach odpowiadające przepisom rozporządzenia (WE) nr 45/2001) zostały dostarczone osobom, których dane dotyczą w skuteczny sposób i w wyczerpującym zakresie. Ponadto, w zależności od struktury zarządzania, którą należy uzgodnić, oraz ról i obowiązków poszczególnych zaangażowanych stron, wniosek dotyczący dyrektywy może w szczególności wymagać, by operator systemu pełnił aktywną rolę w dostarczaniu na jego stronie informacji i innych danych osobom, których dane dotyczą, również „w imieniu" rejestrów przedsiębiorstw. Więcej szczegółowych kwestii można włączyć do aktów delegowanych, w razie takiej konieczności, lub pozostawić ją polityce ochrony danych.

3.10. **Prawo dostępu, prawo do poprawiania i do usuwania**

71. Wniosek powinien zawierać chociaż odniesienie do wymogu utworzenia szczegółowych zasad struktury (w aktach delegowanych) umożliwiającej osobom, których dane dotyczą, wykonanie ich praw. Należy również poczynić odniesienie do możliwości stworzenia modułu ochrony danych i możliwości rozwiązań uwzględniających zasadę ochrony prywatności w fazie projektowania do współpracy pomiędzy organami w zakresie prawa dostępu, a w stosownych przypadkach do „wzmocnienia pozycji osób, których dane dotyczą".

3.11. **Właściwe przepisy**

72. Uznając, że możliwe jest, by Komisja lub inna instytucja/organ UE również przetwarzał dane osobowe w sieci elektronicznej (np. poprzez działania w roli operatora sieci lub poprzez wyszukiwane danych osobowych w tej sieci), należy także poczynić odniesienie do rozporządzenia (WE) nr 45/2001.

73. Należy również wyjaśnić, że dyrektywa 95/46/WE ma zastosowanie do rejestrów biznesowych oraz innych stron działających zgodnie z przepisami krajowymi w państwach członkowskich, podczas gdy rozporządzenie (WE) nr 45/2001 ma zastosowanie do Komisji oraz innych instytucji i organów UE.

3.12. **Przekazywanie danych osobowych państwom trzecim**

74. W odniesieniu do przekazywania danych osobowych przez posiadacza rejestru przedsiębiorstw w UE posiadaczowi rejestru przedsiębiorstw w państwie trzecim, które nie zapewnia odpowiedniego poziomu ochrony danych osobowych, EIOD w pierwszej kolejności podkreśla, że należy odróżnić dwie sytuacje:

— przypadki, w których dane osobowe są już dostępne w rejestrze publicznym (np. poprzez wspólną europejską platformę/punkt dostępu), oraz

— przypadki, w których dane osobowe nie są publiczne dostępne.

75. W pierwszym przypadku art. 26 ust. 1 lit. f) dyrektywy 95/46/WE dopuszcza wyjątek, gdy „przekazanie danych następuje z [publicznego] rejestru", pod warunkiem zastosowania się do kilku warunków. Na przykład jeśli posiadacz rejestru przedsiębiorstw w europejskim kraju chciałby przekazać określony zestaw danych osobowych (np. w związku z rejestracją oddziałów zagranicznych) posiadaczowi rejestru przedsiębiorstw w państwie trzecim, a te same dane byłyby już dostępne publiczne, przekazanie danych powinno być zawsze możliwe, nawet jeśli dane państwo trzecie nie zapewnia odpowiedniego poziomu ochrony.

76. W drugim przypadku EIOD zaleca, by wniosek wyjaśniał, że dane, które nie są publicznie dostępnie, mogą zostać przekazane osobom prawnym lub fizycznym w państwie trzecim, które nie zapewnia odpowiedniego poziomu ochrony, tylko wtedy gdy administrator danych zapewni odpowiednie gwarancje ochrony prywatności i podstawowych praw i wolności osób fizycznych oraz w zakresie wykonywania odpowiadających im praw. Takie gwarancje mogą w szczególności wynikać z odpowiednich klauzul umownych wprowadzonych zgodnie z art. 26 ust. 2 dyrektywy 95/46/WE [1]. W przypadkach, w których takie przekazywanie danych do państw trzecich dotyczy danych regularnie wymienianych pomiędzy rejestrami przedsiębiorstw w dwóch lub kilku państwach UE, lub gdy działanie na poziomie UE jest z innych względów pożądane, negocjacje klauzul umownych mogą również mieć miejsce na poziomie UE (art. 26 ust. 4).

77. EIOD podkreśla, że inne odstępstwa, takie jak to, w którym (art. 26 [ust. 1] lit. d)) „przekazanie danych jest konieczne lub wymagane przez prawo z ważnych względów publicznych lub w celu ustanowienia, wykonania lub obrony tytułu prawnego", nie powinny być wykorzystywane jako uzasadnienie dla systematycznego przekazywania danych do państw trzecich za pośrednictwem sieci elektronicznej.

[1] Jeśli istnieje możliwość, by w niektórych przypadkach Komisja mogła wliczać się do podmiotów, które mogą przekazywać dane do państw trzecich, należy również zamieścić odniesienie do art. 9 ust. 1 i 7 rozporządzenia (WE) nr 45/2001.

3.13. **Odpowiedzialność i ochrona prywatności w fazie projektowania**

78. EIOD zaleca, by wniosek zawierał oddzielne odniesienie do zasady odpowiedzialności ([1]) i starał się ją wdrożyć oraz ustanawiał jasne ramy dla odpowiednich wewnętrznych mechanizmów i systemów kontroli w celu zapewnienia zgodności z zasadami ochrony danych i potwierdzenia tej zgodności, na przykład:

— przeprowadzanie oceny wpływu na prywatność (w tym analiza zagrożeń dla bezpieczeństwa) przed zaprojektowaniem systemu,

— przyjęcie i aktualizacja, stosownie do potrzeb, oficjalnej polityki ochrony danych (zasad wykonawczych), również w odniesieniu do planu bezpieczeństwa,

— przeprowadzanie okresowych kontroli w celu oceny ciągłości w adekwatności polityki ochrony danych i polityki bezpieczeństwa oraz zgodności z ich zasadami,

— udostępnianie (przynajmniej częściowe) wyników tych kontroli w celu zapewnienia stron zainteresowanych o zgodności z zasadami ochrony danych, oraz

— powiadamianie o naruszeniach ochrony danych i innych naruszeniach bezpieczeństwa.

79. Jeśli chodzi o ochronę prywatności w fazie projektowania ([2]), wniosek powinien zawierać odrębne odniesienie do tej zasady oraz urzeczywistnić to zobowiązanie za pomocą konkretnych działań. W szczególności wniosek powinien stanowić, że sieć elektroniczna musi zostać utworzona w sposób bezpieczny i solidny, musi więc z założenia zawierać szereg gwarancji prywatności. Poniżej kilka przykładów potencjalnych gwarancji prywatności w fazie projektowania:

— zdecentralizowane podejście, w którym dane są przechowywane wyłącznie w „głównym" źródle a każdy „dystrybutor" jedynie wyszukuje dane w tym „głównym źródle" (w celu zapewnienia aktualizacji danych),

— automatyczne przetwarzanie, które wyszukuje niespójności i nieścisłości danych,

— ograniczone zdolności wyszukiwania w celu indeksowania jedynie tych danych, które są proporcjonalne i adekwatne do celu,

— inne gwarancje w celu uniemożliwienia/ograniczenia masowego pobierania danych, eksploracji danych, niezgodnych z przeznaczeniem wyszukań oraz w celu zapewnienia odpowiedniego przestrzegania zasady celowości; gwarancje mające na celu wyeliminowanie lub ograniczenie możliwości dla państw trzecich wykorzystania interfejsu wyszukiwania do gromadzenia danych i profilowania osób (np. „captcha" ([3]) lub wymóg rejestracji w celu dokonania płatności),

— wbudowana do systemu funkcja ułatwiająca osobom, których dane dotyczą, skuteczne wykonywanie ich praw; wbudowane funkcje dla rejestrów przedsiębiorstw dla ich wzajemnej koordynacji w zakresie wniosków osób, których dane dotyczą, o udostępnienie danych,

— procedury przetwarzania danych o wnioskodawcach, którzy pobrali informacje z publicznego rejestru bezpiecznie i z poszanowaniem prywatności, oraz

— mechanizmy kontroli/testów.

IV. **WNIOSKI**

80. EIOD popiera cele wniosku. Jego uwagi należy ocenić w świetle tego konstruktywnego podejścia.

81. EIOD podkreśla, że niezbędne gwarancje ochrony danych powinny zostać jasno i oddzielnie określone bezpośrednio w tekście samej dyrektywy, ponieważ uznaje je za istotne elementy. Dodatkowe przepisy dotyczące wdrażania szczegółowych gwarancji można następnie zawrzeć w aktach delegowanych.

82. Kwestie zarządzania, roli, kompetencji i obowiązków należy włączyć do wniosku dotyczącego dyrektywy. W tym celu wniosek dotyczący dyrektywy powinien określić:

— czy sieć elektroniczna będzie prowadzona przez Komisję, czy przez stronę trzecią oraz czy będzie miała scentralizowaną, czy zdecentralizowaną strukturę,

— zadania i obowiązki każdej strony zaangażowanej w przetwarzanie danych i zarządzanie siecią elektroniczną, w tym Komisji, przedstawicieli państw członkowskich, posiadaczy rejestrów przedsiębiorstw w państwach członkowskich i stron trzecich,

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

([2]) Idem.

([3]) „Captcha" to rodzaj testu wykorzystywanego w informatyce jako próba dopilnowania, by odpowiedź nie była generowana przez komputer.

— związek pomiędzy systemem elektronicznym przewidzianym we wniosku a innymi inicjatywami, takimi jak IMI portal e-sprawiedliwości i EBR,

— odrębne i jednoznaczne elementy w celu ustalenia, czy dany podmiot powinien być postrzegany jako „administrator danych" lub „podmiot przetwarzający".

83. Wszelka działalność w zakresie przetwarzania danych za pośrednictwem sieci elektronicznej powinna być oparta na wiążącym instrumencie prawnym, takim jak określony akt Unii przyjęty na solidnej postawie prawnej. Powinno to zostać wyraźnie określone we wniosku dotyczącym dyrektywy.

84. Przepisy dotyczące właściwych przepisów powinny być jasne i zawierać odniesienie do rozporządzenia (WE) nr 45/2001.

85. W odniesieniu do przekazywania danych do państw trzecich, wniosek powinien wyjaśniać, że zasadniczo, z wyjątkiem przypadków mieszczących się w zakresie art. 2 ust. 1 lit. f) dyrektywy 95/46/WE, dane mogą zostać przekazane osobom prawnym lub fizycznym w państwie trzecim, które nie zapewnia odpowiedniego poziomu ochrony, tylko wtedy gdy administrator danych zapewni odpowiednie gwarancje ochrony prywatności i podstawowych praw i wolności osób fizycznych oraz w zakresie wykonywania odpowiadających im praw. Takie gwarancje mogą w szczególności wynikać z odpowiednich klauzul umownych wprowadzonych zgodnie z art. 26 ust. 2 dyrektywy 95/46/WE.

86. Ponadto Komisja powinna starannie ocenić, jakie środki techniczne i organizacyjne podjąć w celu dopilnowania, by ochrona prywatności i danych była „zaprojektowana" w architekturze sieci elektronicznej („ochrona prywatności w fazie projektowania") oraz by odpowiednie kontrole były przeprowadzane w celu zapewnienia zgodności z zasadami ochrony danych i jej potwierdzenia („odpowiedzialność").

87. Poniżej inne zalecenia EIOD:

— wniosek dotyczący dyrektywy powinien jasno określać, że sieć elektroniczna powinna umożliwiać (i) z jednej strony, odrębną ręczną wymianę danych pomiędzy rejestrami przedsiębiorstw; (ii) z drugiej strony, automatyczne przekazywanie danych. Wniosek powinien zostać zmieniony w sposób gwarantujący, że (i) akty delegowane będą w pełni obejmować ręczną i automatyczną wymianę danych; oraz (ii) są objęte wszystkie operacje przetwarzania danych, które mogą dotyczyć danych osobowych (nie tylko przechowywanie i wyszukiwanie); oraz że (iii) odrębne przepisy dotyczące ochrony danych w aktach delegowanych będą również zapewniać praktyczne stosowanie istotnych gwarancji w zakresie ochrony danych,

— wniosek powinien zmienić art. 2 dyrektywy 2009/101/WE w celu wyjaśnienia, które dane osobowe, jeśli którekolwiek, obok imion i nazwisk odnośnych osób należy ujawnić. Należy również wyjaśnić, czy dane dotyczące udziałowców muszą zostać ujawnione. Należy przy tym starannie uwzględnić konieczność przejrzystości i odpowiedniej identyfikacji tych osób, jednocześnie pamiętając o innych przeciwległych aspektach, takich jak konieczność ochrony prawa do ochrony danych osobowych odnośnych osób,

— we wniosku należy wyjaśnić, czy państwa członkowskie mogą ostatecznie udostępnić publicznie więcej informacji za pośrednictwem wspólnego portalu (lub wymienić między sobą więcej informacji) w oparciu o ich własne przepisy krajowe, z uwzględnieniem dodatkowych gwarancji w zakresie ochrony danych,

— wniosek dotyczący dyrektywy powinien w szczególności stanowić, że dane osobowe udostępnione do celów przejrzystości nie zostaną niewłaściwe wykorzystane do dodatkowych, niepowiązanych celów i w tym celu należy wdrożyć techniczne i organizacyjne środki, z uwzględnieniem zasady ochrony prywatności w fazie projektowania,

— wniosek powinien również zawierać szczegółowe gwarancje dostarczania informacji osobom, których dane dotyczą, oraz wymogu tworzenia szczegółowych zasad struktury umożliwiającej osobom, których dane dotyczą, wykonanie praw w aktach delegowanych.

Sporządzono w Brukseli dnia 6 maja 2011 r.

Giovanni BUTTARELLI

Zastępca Europejskiego Inspektora Ochrony Danych