



**00062/10/PL
WP 173**

Opinia 3/2010 w sprawie zasady rozliczalności

Przyjęta w dniu 13 lipca 2010 r.

Grupa robocza została ustanowiona na mocy art. 29 dyrektywy 95/46/WE. Jest ona niezależnym europejskim organem doradczym w zakresie ochrony danych i prywatności. Zadania grupy określone są w art. 30 dyrektywy 95/46/WE i art. 15 dyrektywy 2002/58/WE.

Obsługę sekretariatu zapewnia Dyrekcja C (Prawa Podstawowe i Obywatelstwo Unii Europejskiej) Dyrekcji Generalnej ds. Sprawiedliwości Komisji Europejskiej, B-1049 Bruksela, Belgia, Biuro nr LX-46 01/190.

Strona internetowa: http://ec.europa.eu/justice/policies/privacy/index_en.htm

STRESZCZENIE

Unijne zasady ochrony danych i związane z nimi obowiązki są często niewystarczająco odzwierciedlone w konkretnych wewnętrznych środkach i praktykach. Dopóki ochrona danych nie stanie się częścią wspólnych wartości i praktyk organizacji, a odpowiedzialności za nie zostaną wyraźnie przydzielone, nie będzie możliwe zagwarantowanie skutecznego przestrzegania zasad ochrony danych, a problemy w dziedzinie ochrony danych nadal będą miały miejsce.

Aby wspierać ochronę danych w praktyce, w ramach prawnych UE niezbędne są dodatkowe narzędzia. W związku z powyższym celem niniejszej opinii jest doradzenie Komisji, w jaki sposób zmienić dyrektywę o ochronie danych. W szczególności, niniejsza opinia przedstawia konkretne propozycje w odniesieniu do zasady rozliczalności, która wymagałaby od administratorów danych wprowadzenia stosownych i skutecznych środków w celu zapewnienia, że zasady i związane z nimi obowiązki ustanowione w dyrektywie są przestrzegane oraz na żądanie wykazania tego przed organami nadzoru. Powinno to przyczynić się do przeniesienia ochrony danych z „teorii do praktyki” i pomóc organom ochrony danych w ich nadzorowaniu i przestrzeganiu.

Opinia zawiera sugestie, w jaki sposób zapewnić, aby zasada rozliczalności dawała pewność prawną, pozwalając jednocześnie na skalowalność (tj. umożliwiała określenie konkretnych środków, które należy zastosować zależnie od ryzyka związanego z przetwarzaniem i rodzaju przetwarzanych danych). Następnie omówiono, jak wymieniona zasada może wpłynąć na inne dziedziny, w tym międzynarodowe przesyłanie danych, wymagania powiadamiania, sankcje i ostatecznie również programy certyfikacji czy certyfikaty bezpieczeństwa.

Grupa robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych

powołana dyrektywą 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r.,

uwzględniając art. 29 i 30 ust. 1 lit. a) i ust. 3 tej dyrektywy oraz art. 15 ust. 3 dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r.,

uwzględniając swój regulamin,

przyjmuje niniejszą opinię:

1. WPROWADZENIE

1. Ochronę danych należy przenieść z „teorii do praktyki”. Wymogi prawne należy zmienić w rzeczywiste środki ochrony danych. W celu wsparcia ochrony danych w praktyce, ramy prawne UE w zakresie ochrony danych wymagają dodatkowych mechanizmów. W dyskusjach o przyszłości ram ochrony danych na poziomie europejskim i globalnym, zaproponowano mechanizmy oparte na rozliczalności jako sposób zachęcenia administratorów danych do stosowania praktycznych narzędzi do skutecznej ochrony danych.
2. W swoim dokumencie o przyszłości kwestii prywatności (WP 168) z grudnia 2009 r., grupa robocza art. 29 wyraziła pogląd, że obecne ramy prawne nie są wystarczające by zapewnić, że wymogi dotyczące ochrony danych przekładają się na skuteczne mechanizmy zapewniające rzeczywistą ochronę. Aby poprawić tę sytuację, grupa robocza art. 29 zaproponowała, żeby Komisja rozważyła mechanizmy oparte na rozliczalności, ze szczególnym naciskiem na możliwość włączenia zasady „rozliczalności” do zmienionej dyrektywy o ochronie danych¹. Odnośna zasada wzmocniłaby rolę administratora danych i zwiększyła jego odpowiedzialność.
3. Podsumowując, umocowana prawnie zasada rozliczalności w sposób wyraźny wymagałaby, aby administratorzy danych stosowali właściwe i skuteczne środki w celu wprowadzenia w życie zasad i związanych z nimi obowiązków zawartych w dyrektywie i wykazywali to na żądanie. W praktyce powinno to przełożyć się

¹ „Aby rozwiązać ten problem, właściwe byłoby wprowadzić w kompleksowe ramy zasadę odpowiedzialności. Zgodnie z tą zasadą, administratorzy danych byłiby zobowiązani do podjęcia niezbędnych środków by zapewnić, że przy przetwarzaniu danych osobowych stosowane są podstawowe zasady i związane z nimi obowiązki zawarte w obowiązującej dyrektywie. Takie przepisy wzmocniłyby potrzebę ustanowienia strategii i mechanizmów w celu przestrzegania podstawowych zasad i związanych z nimi obowiązków odnośnej dyrektywy. Działania te wzmocniłyby potrzebę podjęcia skutecznych kroków, których rezultatem byłoby wewnętrzne skuteczne wdrożenie obowiązków i zasad włączonych obecnie do dyrektywy. Ponadto, zasada odpowiedzialności wymagałaby od administratorów danych korzystania z niezbędnych mechanizmów wewnętrznych w celu wykazania zgodności zainteresowanym podmiotom zewnętrznym, w tym krajowym organom ochrony danych. Wynikająca z tego potrzeba przedstawienia dowodu odpowiednich środków podjętych w celu zapewnienia przestrzegania przepisów znacznie ułatwi egzekwowanie mających zastosowanie przepisów” (WP168, ust. 79. Więcej informacji w ust.74-78).

na skalowalne programy mające na celu wdrożenie istniejących zasad ochrony danych (czasem określane jako „programy zgodności”) W uzupełnieniu do tej zasady można byłoby ustanowić szczególne wymagania dodatkowe mające na celu wprowadzenie w życie zabezpieczeń w zakresie ochrony danych lub zapewnienie ich skuteczności. Jednym z przykładów może być przepis wymagający przeprowadzenia oceny skutków w zakresie ochrony prywatności dla operacji przetwarzania danych o podwyższonym ryzyku.

4. Niniejsza opinia ma na celu rozwinięcie wcześniejszego wkładu grupy roboczej art. 29 na ten temat, zawartego w opinii w sprawie przyszłości kwestii prywatności, aby doradzić Komisji co do obecnie trwającego przeglądu dyrektywy 95/46. W tym celu niniejsza opinia dzieli się na cztery części: W pierwszej części omówiona jest potrzeba wzmocnienia przez administratorów danych ich rozwiązań wewnętrznych (strategii i procedur) by zapewnić, że cały proces przetwarzania jest przeprowadzany zgodnie z obowiązującymi zasadami; w tej części omówiony został również sposób, w jaki systemy oparte na rozliczalności mogą przyczynić się do realizacji wymienionego celu. Następnie przedstawiono analizę ewentualnej struktury architektury prawnej systemu opartego na rozliczalności oraz precedensów w dziedzinie ochrony danych i innych dziedzinach. W części drugiej przedstawiona została konkretna propozycja dotycząca zasady rozliczalności oraz podano racjonalne uzasadnienie dla różnych aspektów tej propozycji. W części trzeciej omówiono różne elementy związane z systemem prawnym, obejmującym ogólny system rozliczalności. Dalej przedstawiono argumenty, dlaczego taka propozycja musi dawać pewność prawną, a jednocześnie mieć dostatecznie szeroki zakres, aby umożliwić skalowalność (pozwalając tym samym na określenie konkretnych środków i weryfikację metod, które mają być zastosowane w zależności od ryzyka przetwarzania i rodzaju przetwarzanych danych). Następnie omówiono aspekty związane z powyższym, takie jak powiązania z przekazami międzynarodowymi, przedstawia się także opis korzyści, jakie daje mechanizm oparty na rozliczalności organom ochrony danych oraz założenia co do roli, jaką mogłaby odegrać certyfikacja.

II. ROZLICZALNOŚĆ: CELE, ARCHITEKTURA PRAWNA, PRECEDENSY I TERMINOLOGIA

II.1 Rozliczalność jako siła napędowa dla skutecznego wdrożenia zasad ochrony danych

5. Obecnie zaobserwować można rosnącą potrzebę zapewnienia przez administratorów danych skutecznych środków, umożliwiających rzeczywistą ochronę danych oraz coraz większe zainteresowanie tą kwestią i zainteresowanie. Dzieje się tak z kilku powodów, które zostały omówione poniżej.
6. Po pierwsze, jesteśmy świadkami tak zwanego efektu „potopu danych”, gdzie ciągle wzrasta ilość istniejących danych osobowych, które są przetwarzane i przekazywane dalej. Temu zjawisku sprzyjają zarówno rozwój technologiczny, tj. wzrost systemów informacji i komunikacji, jak i rosnąca zdolność jednostek do interaktywnego wykorzystania technologii. Ze względu na to, że coraz więcej

danych jest dostępnych i przekazywanych, ryzyko naruszenia bezpieczeństwa danych również wzrasta. to również podkreśla potrzebę stosowania przez administratorów danych, zarówno w sektorze publicznym jak i prywatnym, rzeczywistych i skutecznych mechanizmów wewnętrznych w celu zapewnienia ochrony danych osobowych.

7. Po drugie, ciągłemu wzrostowi ilości danych osobowych towarzyszy wzrost ich wartości w kategoriach społecznych, politycznych i gospodarczych. W pewnych sektorach, szczególnie w środowisku on-line, dane osobowe stały się faktyczną walutą, za którą w zamian otrzymuje się treści on-line. W tym samym czasie, ze społecznego punktu widzenia, obserwuje się wzrastające uznanie dla ochrony danych jako wartości społecznej. Podsumowując – ze względu na to, że dane osobowe stają się bardziej wartościowe dla administratorów danych w różnych sektorach, obywatele, konsumenci i ogół społeczeństwa stają się także coraz bardziej świadomi ich znaczenia. To z kolei wzmacnia potrzebę zastosowania bardziej rygorystycznych środków w celu ich ochrony.
8. Z powyższego wynika zatem, że naruszenie bezpieczeństwa danych osobowych może mieć istotny negatywny wpływ dla administratorów danych w sektorze publicznym i prywatnym. Potencjalne usterki w administracji elektronicznej i elektronicznych usługach opieki zdrowotnej będą miały poważne skutki zarówno pod względem ekonomicznym jak i – w sposób szczególny – w zakresie wiarygodności. Tak więc minimalizowanie ryzyka, budowanie i podtrzymywanie dobrej opinii, oraz dbałość o zaufanie obywateli i konsumentów stają się decydujące dla administratorów danych we wszystkich sektorach.
9. Podsumowując, powyższe pokazuje pilną potrzebę, aby administratorzy danych stosowali rzeczywiste środki ochrony danych mające na celu zapewnienie dobrego zarządzania w zakresie ochrony danych, przy jednoczesnym minimalizowaniu ryzyka prawnego i gospodarczego, a także ryzyka naruszenia dobrej opinii, mogących wynikać z niewłaściwych praktyk w zakresie ochrony danych. Jak przedstawiono poniżej, mechanizmy oparte na rozliczalności dążą do zrealizowania tych celów.

II.2 Ewentualna ogólna architektura prawna mechanizmów opartych na rozliczalności.

10. W tym kontekście istotnym zagadnieniem do omówienia jest sposób, w jaki ramy prawne mogłyby zachęcić administratorów danych do podjęcia środków zapewniających rzeczywistą ochronę w praktyce. Innymi słowy dotyczy to możliwej struktury architektury prawnej systemów opartych na rozliczalności.
11. W uwadze wstępnej przed omówieniem takiej architektury należy podkreślić, że na początku takie systemy nie zmieniają w żaden sposób podstawowych zasad ochrony danych, ani nie mają na nie wpływu, ale są one zaprojektowane tak, aby te zasady lepiej funkcjonowały.
12. Jednym sposobem, aby spowodować, żeby administratorzy danych wprowadzili takie środki, byłoby dodanie zasady rozliczalności do zmienionej wersji dyrektywy. Oczekiwane efekty takiego przepisu obejmowałyby wdrożenie

wewnętrznych środków i procedur, wprowadzających w życie istniejące zasady ochrony danych, zapewnienie ich skuteczności i wprowadzenie obowiązku wykazania tego na żądanie organów ochrony danych. Jak opisano poniżej, rodzaje procedur i mechanizmów różniłyby się w zależności od ryzyka związanego z przetwarzaniem i charakterem danych.

13. Ponadto, można by zastanowić się nad szczególnymi wymogami, takimi jak obowiązek przeprowadzenia oceny skutków w zakresie ochrony prywatności w poszczególnych przypadkach, lub wyznaczeniem inspektorów ds. ochrony danych. Te szczególne wymogi mogłyby uzupełniać ogólną zasadę rozliczalności.
14. Grupa robocza art. 29 uznaje, że administratorzy danych mogą chcieć wdrożyć strategie i procedury, które nie są ściśle przewidziane w ustawodawstwie dotyczącym ochrony danych. Na przykład administrator danych może chcieć zobowiązać się do odpowiedzi na wnioski o udzielenie dostępu w bardzo krótkim okresie czasu, nawet jeśli prawo przewiduje pewną elastyczność. Może on także chcieć zobowiązać się do udzielenia odpowiedzi na wnioski o udzielenie dostępu jednocześnie w trybie on- i off-line, aby zapewnić szybki i skuteczny odbiór takich informacji. Można także wyobrazić sobie sytuację, w której administrator danych chce wyjść poza minimalne wymogi zawarte w ogólnych ramach prawnych. Na przykład administrator danych może podjąć decyzję o wyznaczeniu inspektora ds. ochrony danych, nawet jeśli nie jest to obowiązujące w ramach istniejących przepisów. Administrator danych może również chcieć zaangażować osobę trzecią do przeprowadzenia audytu na podstawie *wszystkich* swoich operacji przetwarzania danych w celu dokonania oceny, czy są one zgodne z ramami prawnymi w zakresie ochrony danych. Grupa robocza art. 29 pochwala te inicjatywy i zachęca, aby nowe ramy prawne w zakresie ochrony danych stanowiły impuls dla administratorów danych do wprowadzania w życie takich inicjatyw.
15. Zgodnie z powyższym „architektura prawna” mechanizmów rozliczalności przewidywałaby dwa poziomy: pierwszy poziom obejmowałby podstawowy wymóg prawny, wiążący dla *wszystkich* administratorów danych. Treść wymogu zawierałaby dwa elementy: wdrożenie środków lub procedur i gromadzenie odpowiednich dowodów. Wymagania szczególne mogłyby uzupełnić ten pierwszy poziom. Drugi poziom obejmowałby dobrowolne systemy rozliczalności, które wychodzą poza minimalne wymogi prawne, w takim zakresie jak podstawowe zasady ochrony danych (zapewnianie wyższych gwarancji niż te wymagane w ramach obowiązujących zasad), lub pod względem sposobu wdrożenia albo zapewnienia skuteczności środków (wdrożenie wymogów, które wykraczają poza poziom minimalny). Uwzględniając znaczenie i korzyści takich systemów, niniejsza opinia ma przede wszystkim na uwadze wymóg pierwszego poziomu, w szczególności ogólną zasadę rozliczalności.

II.3 Zasada rozliczalności w dziedzinie ochrony danych i innych dziedzinach oraz terminologia

Precedensy

16. Grupa robocza art. 29 zauważa, że zasada rozliczalności jako taka nie jest nowa. Jej wyraźne uznanie można zauważyć w wytycznych Organizacji Współpracy Gospodarczej i Rozwoju (OECD) dotyczących ochrony prywatności przyjętych w 1980 r. Zgodnie z zawartą w nich zasadą rozliczalności: „Administrator danych powinien odpowiadać za przestrzeganie środków, które nadają skuteczność [istotnym] zasadom wymienionym powyżej.”
17. W ostatnim czasie powyższa zasada została wyraźnie włączona do międzynarodowych standardów madryckich opracowanych przez Międzynarodową Konferencję Komisarzy ds. Ochrony Danych i Prywatności². Została także włączona do najnowszego projektu normy ISO 29100 ustanawiającej zasady ramowe dotyczące prywatności i jest jedną z głównych pojęć ramowych zasad prywatności APEC i odnośnych przepisów prywatności transgranicznej³.
18. Z perspektywy przepisów prawnych grupa robocza art. 29 zauważa, że do rozliczalności odnoszą się kanadyjskie *Fair Information Principles* (zasady uczciwej informacji) zawarte w *Personal Information Protection and Electronic Documents Act* (kanadyjskiej ustawie o ochronie danych osobowych i dokumentach elektronicznych). Pierwsza zasada, między innymi, wymaga opracowania i wdrożenia strategii i praktyk mających na celu utrzymanie 10 zasad uczciwej informacji, w tym wdrożenia procedur w celu ochrony danych osobowych, oraz ustanowienia procedur otrzymywania skarg i pytań i odpowiadania na nie.
19. Ponadto, grupa robocza art. 29 podkreśla, że zasadę rozliczalności odzwierciedlają wiążące przepisy dla przedsiębiorstw („BCR”), które są wykorzystywane w kontekście międzynarodowego przekazu danych. W rzeczywistości BCR są kodeksami praktyk, ustanowionych i przestrzeganych przez organizacje międzynarodowe, zawierającymi wewnętrzne środki przeznaczone do wprowadzenia w życie zasad ochrony danych (takie jak audyt, programy szkoleniowe, sieć inspektorów ds. prywatności, system rozpatrywania skarg). Po przeglądzie przez krajowe organy ochrony danych, można uznać, że BCR zapewniają odpowiednie zabezpieczenie w przypadku przesyłania lub określonych kategorii przesyłania danych osobowych pomiędzy przedsiębiorstwami, które są częścią tej samej grupy przedsiębiorstw i są związane przez wiążące zasady dla przedsiębiorstw, dawne art. 25 i 26 ust. 2 dyrektywy 95/46.

² Osoba odpowiedzialna: „a) wprowadza wszystkie niezbędne środki w celu przestrzegania zasad i zobowiązań ustanowionych w niniejszym dokumencie i w mającym zastosowanie ustawodawstwie krajowym, oraz b) korzysta z wszystkich niezbędnych mechanizmów wewnętrznych w celu wykazania takiego przestrzegania zarówno wobec podmiotów danych, jak i organów nadzoru wykonujących swoje zadania, jak ustanowiono w sekcji 23.”

³ Ponadto, w inicjatywę badania skutków zasady odpowiedzialności w odniesieniu do ochrony danych i prywatności zaangażowane jest Centrum Polityki Informacyjnej i Przywództwa. Zob.: www.informationpolicycentre.com

20. Na zewnątrz świata ochrony danych, istnieje kilka przykładów rozliczalności – takich jak program wyszczególniający strategie i procedury administratorów danych w celu zapewnienia zgodności z przepisami ustawowymi i wykonawczymi. Na przykład, programy zgodności są obowiązkowe na mocy przepisów wykonawczych dotyczących usług finansowych. W innych przypadkach, programy zgodności nie są obowiązkowe, ale zachęca się do nich, jak np. w dziedzinie prawa konkurencji. Na przykład w Kanadzie komisarz ds. konkurencji opracował szczegółowe uregulowania dotyczące programów zgodności dla przedsiębiorstw. Decyzja w sprawie stosowania takiego programu podejmowana jest przez przedsiębiorstwa dobrowolnie. Pomimo to, kanadyjski komisarz ds. konkurencji podkreśla wagę zgodności jako narzędzia ograniczenia ryzyka, oraz podkreśla korzyści prawne, gospodarcze oraz w zakresie wiarygodności⁴.

Terminologia

21. Termin „rozliczalność” (ang. *accountability*) pochodzi z kultury anglosaskiej, gdzie jest w powszechnym użyciu, a jego znaczenie jest szeroko rozumiane – nawet jeśli stworzenie dokładnej definicji „rozliczalności” w praktyce byłoby trudne. W ujęciu ogólnym termin ten wyraża sposób wykonywania odpowiedzialności i umożliwienie stosownej weryfikacji. Odpowiedzialność (ang. *responsibility*) i rozliczalność (ang. *accountability*) stanowią dwie strony tego samego medalu i są istotnymi składnikami dobrego zarządzania. Dostatecznie zaufanie można rozwinąć jedynie, gdy wykaże się, że odpowiedzialność skutecznie funkcjonuje w praktyce.
22. W większości języków europejskich, przede wszystkim ze względu na różnice w systemach prawnych, nie jest łatwo znaleźć odpowiednik dla słowa „rozliczalność”. W wyniku tego istnieje wysokie ryzyko różnych interpretacji tego terminu, a zatem i brak harmonizacji. Inne słowa, które sugerowano jako oddające znaczenie rozliczalności to „reinforced responsibility” (wzmocniona odpowiedzialność), „assurance” (zabezpieczenie, gwarancja), „reliability” (rzetelność), „trustworthiness” (wiarygodność), a w języku francuskim „obligation de rendre des comptes” (obowiązek zdawania sprawozdań) itp. Można również zasugerować, że rozliczalność odnosi się do „wdrożenia zasad ochrony danych”.
23. W tym dokumencie zatem koncentrujemy się na środkach, które powinno się podjąć lub wprowadzić w celu zapewnienia przestrzegania przepisów w dziedzinie ochrony danych. Odniesienia do rozliczalności należy zatem rozumieć w znaczeniu nadanym w niniejszej opinii, bez uszczerbku dla innych sformułowań, które być może dokładniej odzwierciedlają pojęcie przedstawione w niniejszym dokumencie. Z tego właśnie powodu w niniejszym dokumencie nie przykładamy głównej wagi do terminów, lecz w sposób pragmatyczny koncentruje się on bardziej na środkach, które należy podjąć, niż na samym pojęciu.

⁴ www.bureaudelaconcurrency.gc.ca/eic/site/cb-bc.nsf/eng/02732.html.

III. PROPOZYCJA DOTYCZĄCA OGÓLNEGO PRZEPISU W SPRAWIE ROZLICZALNOŚCI

III.1 Przepis ogólny potwierdzający i wzmacniający odpowiedzialność (*responsibility*) administratorów danych

24. Grupa robocza art. 29 rozważyła możliwość wprowadzenia rozwiązań opartych na rozliczalności do nowych kompleksowych ram prawnych dotyczących ochrony danych, w świetle uwag przedstawionych w sekcji I.
25. W wyniku powyższego, grupa potwierdziła swoje stanowisko wcześniej wyrażone w opinii o przyszłości kwestii prywatności, że ogólna zasada rozliczalności powinna zostać włączona do nowych kompleksowych ram prawnych. Celem takiego przepisu byłoby potwierdzenie i wzmocnienie odpowiedzialności administratorów danych w odniesieniu do przetwarzania danych osobowych. Pozostaje to bez uszczerbku dla możliwości uzupełnienia tej zasady konkretnymi środkami dotyczącymi rozliczalności.
26. Nowy przepis byłby zgodny z przepisami szczegółowymi, które już istnieją w obecnych ramach prawnych. Można się w szczególności odnieść do art. 6 dyrektywy 95/46/WE, który określa zasady dotyczące jakości danych w ust. 1 i gdzie wspomina się (ust. 2), że „na administratorze danych spoczywa obowiązek zapewnienia przestrzegania przepisów ust. 1”. Przepis ten byłby również zgodny z art. 17 ust. 1, który wymaga od administratorów danych wprowadzenia środków o charakterze zarówno technicznym jak i organizacyjnym. W rzeczy samej, przepis ogólny dotyczący rozliczalności w jeszcze większym stopniu skłaniałby administratorów danych do wprowadzenia wymogów ochronnych określonych w art. 17 dodatkowo do wymogów ustanowionych w pozostałych przepisach.

III.2 Konkretnie propozycje dotyczące ogólnej zasady rozliczalności.

27. Nowy przepis miałby na celu wspieranie przyjęcia konkretnych i praktycznych środków, zmieniających ogólne zasady ochrony danych w konkretne strategie i procedury, określone na poziomie administratora zgodnie ze stosownymi przepisami ustawowymi i wykonawczymi. Administrator powinien także zapewnić skuteczność podjętych środków i na żądanie wykazać, że podjął stosowne działania.
28. W uproszczeniu – taki ogólny przepis koncentrowałby się na dwóch głównych elementach:
- (i) wymaganiu podjęcia przez administratora właściwych i skutecznych środków do wdrożenia zasad ochrony danych,
 - (ii) wymaganiu wykazania na żądanie, że właściwe i skuteczne środki zostały podjęte. Zatem administrator danych musi przedstawić dowody w związku z powyższym punktem (i).
29. Obowiązek ten powinien obejmować wszystkich administratorów i wszystkie sytuacje.

30. Pierwszym elementem tego obowiązku byłoby zobowiązanie administratorów danych do wprowadzenia odpowiednich środków. Rodzaje środków nie byłyby wyszczególnione w tekście ogólnego przepisu dotyczącego rozliczalności. Późniejsze wytyczne podane przez krajowe organy ochrony danych, przez grupę roboczą art. 29 lub przez Komisję (za pośrednictwem procedur komitetowych) mogłyby wyszczególnić, w pewnych przypadkach, minimalny zestaw szczególnych środków, aby środki te można było uznać za właściwe. Jednym z przykładów takich środków byłoby przyjęcie w pewnych przypadkach wewnętrznych strategii i procesów niezbędnych do wdrożenia zasad ochrony danych, które odzwierciedlałyby stosowne przepisy ustawowe i wykonawcze.
31. Wdrożenie takich środków i procesów można także skutecznie przeprowadzić poprzez przydzielenie odpowiedzialności i szkolenie personelu zaangażowanego w operacje przetwarzania. W szczególności, zgodnie z art. 18 przedmiotowej dyrektywy, należy zachęcać administratorów danych do wyznaczenia urzędników odpowiedzialnych za ochronę danych osobowych. W każdym razie należy zachęcać do przydzielania odpowiedzialności na różnych poziomach organizacji w celu zapewnienia, że odpowiedzialności te są wykonywane.
32. W odniesieniu do przesyłania danych osobowych poza Unię Europejską, administratorzy danych powinni przyjąć i wdrożyć odpowiednie środki, takie jak w przypadku BCR, aby spełnić wymóg „zalecenia odpowiedniego zabezpieczenia” ustanowionego w art. 26 dyrektywy.
33. Administratorzy powinni także zapewnić, aby praktyczne środki wdrożone w celu przestrzegania zasad ochrony danych były skuteczne. W przypadku większych, bardziej skomplikowanych lub obciążonych większym ryzykiem operacji przetwarzania danych, skuteczność przyjętych środków powinna być regularnie sprawdzana. Istnieją różne sposoby oceny skuteczności środków, lub jej braku: monitorowanie, audyty wewnętrzne i zewnętrzne, itp.
34. Zgodnie z powyższymi uwagami grupa robocza art. 29 rozważyła sformułowanie konkretnego przepisu, który mógłby zostać wprowadzony do kompleksowych ram prawnych i brzmieć następująco:

„Artykuł X – Wdrożenie zasad ochrony danych osobowych

1. *Administrator danych wprowadza odpowiednie i skuteczne środki, aby zapewnić, że zasady i obowiązki ustanowione w dyrektywie są przestrzegane.*
2. *Administrator danych wykazuje przestrzeganie ust. 1 na żądanie organów nadzoru.*

IV. OMÓWIENIE RÓŻNYCH ELEMENTÓW POWIĄZANYCH Z OGÓLNĄ ZASADĄ ROZLICZALNOŚCI.

IV. 1. Wzmacnianie istniejących obowiązków

35. Grupa robocza art. 29 zauważa, że niektórzy administratorzy danych mogą postrzegać ogólną zasadę rozliczalności jako nałożenie nowych uciążliwych

wymogów prawnych na administratorów danych, w szczególności biorąc pod uwagę obecną sytuację gospodarczą UE, która stanowi duże wyzwanie. Byłoby to jednak błędem.

36. Grupa robocza art. 29 pragnie podkreślić, że większość wymogów ustanowionych w tym nowym przepisie w zasadzie już istnieje – pomimo, że mniej wyraźnie – w obowiązujących przepisach ustawowych. W rezultacie, administratorzy danych są już obecnie zobowiązani do przestrzegania zasad i obowiązków ustanowionych w dyrektywie na mocy istniejących ram prawnych. W celu dopełnienia tego obowiązku, z natury rzeczy konieczne jest ustanowienie procedur związanych z ochroną danych i ich ewentualną weryfikacją. Z tej perspektywy, przepis dotyczący rozliczalności nie stanowi wielkiej nowości i w zasadzie, nie nakłada wymogów, które nie byłyby już dorozumiane w istniejących przepisach. Podsumowując, nowy przepis nie ma na celu podporządkowania administratorów danych nowym zasadom, lecz raczej faktyczne zapewnienie skutecznego przestrzegania przepisów już istniejących.
37. W rzeczywistości, nieco podobna inicjatywa legislacyjna powstała podczas zmiany dyrektywy 2002/58 w 2009 r.⁵. W tym przypadku wspomniany akt nakłada obowiązek wdrożenia polityki ochrony, mianowicie „zapewnić wdrożenie polityki bezpieczeństwa w odniesieniu do przetwarzania danych osobowych”. Zatem, w odniesieniu do przepisów dotyczących bezpieczeństwa w tej dyrektywie ustawodawca zdecydował, że niezbędne było wprowadzenie wyraźnego wymogu stworzenie i wdrożenie polityki bezpieczeństwa. Ponadto, art. 18 dyrektywy 1995/46, odnoszący się do wyznaczenia urzędników ds. ochrony danych, jak i system wiążących przepisów dla przedsiębiorstw wymieniony powyżej, już stanowią przykłady praktycznych środków, które mogą przyjąć administratorzy danych.
38. Z powyższymi uwagami wiąże się kwestia skutków przestrzegania (lub też nieprzestrzegania) zasady rozliczalności. Grupa robocza art. 29 podkreśla, że dopełnienie zasady rozliczalności niekoniecznie oznacza, że administrator danych przestrzega podstawowych zasad ustanowionych w dyrektywie, tj. nie pozwala ono na wysnucie domniemania prawnego co do przestrzegania, ani też nie zastępuje żadnej z wymienionych zasad. Możliwe jest, że administrator danych wdrożył i sprawdził wprowadzone środki, ale wciąż może okazać się, że naruszył zasady ochrony danych. Zatem przyjęcie środków w celu przestrzegania zasad nie może w żadnym przypadku wyłączyć administratorów danych z podlegania działaniom służącym egzekwowaniu przepisów przez organy ochrony danych. W praktyce, istnieje większe prawdopodobieństwo, że administratorzy danych sektora publicznego i prywatnego, którzy przyjęli środki w ramach solidnie przygotowanych programów zgodności, przestrzegają obowiązujących przepisów. Istotnie, ze względu na wprowadzenie przez nich w życie skutecznych środków ukierunkowanych na przestrzeganie podstawowych zasad ochrony danych,

⁵ Dyrektywa Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r. zmieniająca dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów.

powinno być mniej prawdopodobne, że naruszyli oni obowiązujące przepisy. Zatem przy określaniu sankcji związanych z naruszeniem ochrony danych, organy ochrony danych mogłyby uwzględniać wdrożenie środków i ich weryfikację (lub ich brak).

IV.2 Odpowiednie środki w celu wdrożenia przepisów dyrektywy

39. Przepis dotyczący rozliczalności zobowiązywałby administratorów danych do określenia i wdrożenia niezbędnych środków w celu zapewnienia przestrzegania zasad i obowiązków określonych w dyrektywie, oraz do okresowego weryfikowania ich skuteczności.
40. Zaproponowana ogólna zasada rozliczalności celowo unika sprecyzowania rodzajów środków, jakie miałyby być wdrożone. Prowadzi to do dwóch powiązanych ze sobą zasadniczych pytań, mianowicie: (i) które wspólne środki spełniłyby zasadę rozliczalności? (ii) jak dostosować środki i ich zakres do szczególnych okoliczności?

Środki: przykład.

41. Grupa robocza art. 29 uważa, że wspólne środki rozliczalności mogą obejmować następujący niewyczerpujący wykaz:

- ustanowienie wewnętrznych procedur *przed* wprowadzeniem nowych operacji przetwarzania danych osobowych (przegląd wewnętrzny, ocena),⁶
- utworzenie pisemnych i wiążących strategii w zakresie ochrony danych, które miałyby być brane pod uwagę i stosowane w nowych procesach przetwarzania danych (np. przestrzeganie zasad jakości danych, zawiadomienia, zasady bezpieczeństwa, dostępu itp.); powinny one być dostępne dla podmiotów danych,
- przyporządkowywanie procedur w celu zapewnienia właściwego określenia wszystkich operacji przetwarzania danych i prowadzenie spisu operacji przetwarzania danych,
- wyznaczenie inspektora ds. ochrony danych i innych osób odpowiedzialnych za ochronę danych,
- zapewnienie członkom personelu odpowiednich szkoleń i doskonalenia w zakresie ochrony danych; Oferta ta powinna to obejmować przede wszystkim osoby przetwarzające dane lub które są za to odpowiedzialne (np. dyrektorów ds. zasobów ludzkich), lecz także menedżerów ds. informatyki, programistów i dyrektorów jednostek gospodarczych. Należy przydzielić wystarczające środki na zarządzanie prywatnością itp.,
- utworzenie procedur do zarządzania dostępem, wnioskami o poprawki bądź o usunięcie, które powinny być przejrzyste dla podmiotów danych,
- ustanowienie wewnętrznego mechanizmu rozpatrywania skarg,
- ustanowienie wewnętrznych procedur skutecznego zarządzania przypadkami naruszenia bezpieczeństwa i zgłaszania takich naruszeń,

⁶ W celu dostosowania istniejących procesów przetwarzania danych do prawa potrzebny byłby okres przejściowy.

- przeprowadzanie ocen skutków w zakresie ochrony prywatności w szczególnych okolicznościach,
 - wdrożenie lub nadzorowanie procedur weryfikacji w celu zapewnienia, że wszystkie środki nie tylko istnieją w formie pisemnej, lecz są również stosowane i funkcjonują w praktyce (audyty wewnętrzne i zewnętrzne itp.).
42. Można przewidzieć także podejście uzupełniające do ogólnej zasady rozliczalności. W myśl takiego podejścia ramy prawne obejmowałyby nie tylko ogólną zasadę rozliczalności, lecz także przykładowy wykaz środków, które można byłoby promować na poziomie krajowym⁷. Przepis taki mógłby stanowić przykładowy niewyczerpujący wykaz środków, który stanowiłby „niezbędnik” dla administratorów danych. Zawierałby wytyczne dla administratorów danych w odniesieniu do tego, co stanowiłoby, w zależności od przypadku, właściwe środki, które administrator powinien przyjąć. Powyższy wykaz przykładowy oczywiście jedynie towarzyszyłby ogólnemu obowiązkowi prawnemu przyjęcia odpowiednich środków.

Określanie skali środków

⁷ Na przykład międzynarodowe standardy przyjęte w Madrycie przez organy ochrony danych zawierają w swoim artykule 22 przepis dotyczący środków proaktywnych, który brzmi następująco: „Państwo powinno zachęcać, za pośrednictwem prawa krajowego, aby osoby zaangażowane na jakimkolwiek etapie w przetwarzanie, wprowadzały środki służące promowaniu pełniejszego przestrzegania obowiązujących przepisów dotyczących ochrony prywatności w odniesieniu do przetwarzania danych osobowych. Takie działania mogłyby obejmować m. in.:

- a) Wdrożenie procedur zapobiegania naruszeniom lub ich wykrywania, które mogłoby być oparte o standardowe modele zarządzania bezpieczeństwem informacji.
- b) Wyznaczenie jednego lub więcej inspektorów ds. ochrony danych lub prywatności o odpowiednich kwalifikacjach, zasobach i uprawnieniach do wykonywania funkcji nadzorczych w sposób właściwy.
- c) Okresowe wprowadzanie szkoleń, kształcenia i programów zwiększających świadomość wśród członków organizacji, które miałyby na celu zwiększenie zrozumienia obowiązujących praw dotyczących ochrony prywatności w odniesieniu do przetwarzania danych osobowych, jak i procedur ustanowionych przez organizacje w tym celu.
- d) Okresowe przeprowadzanie przejrzystych audytów przez wykwalifikowane i niezależne osoby w celu sprawdzenia przestrzegania obowiązujących przepisów dotyczących ochrony prywatności w odniesieniu do przetwarzania danych osobowych, jak i procedur ustanowionych w tym celu przez organizację celu.
- e) Przystosowanie systemów danych lub technologii do przetwarzania danych osobowych do obowiązującego prawa dotyczącego ochrony prywatności w odniesieniu do przetwarzania danych osobowych, w szczególności w czasie podejmowania decyzji co do ich technicznych specyfikacji, opracowania i wdrożenia.
- f) Wprowadzenie ocen skutków w odniesieniu do ochrony danych prywatnych przed wdrożeniem nowych systemów informacyjnych lub technologii do przetwarzania danych osobowych, oraz przed wprowadzeniem w życie jakichkolwiek nowych metod przetwarzania danych osobowych lub istotnych zmian w obecnym sposobie przetwarzania.
- g) Przyjęcie kodeksów postępowania, których stosowanie jest wiążące, oraz które zawierają elementy pozwalające na pomiar skuteczności pod względem przestrzegania i poziomu ochrony danych osobowych, oraz które ustanawiają skuteczne środki w przypadku nieprzestrzegania.
- h) Wdrożenie planu reagowania, który ustanawia wskazówki dotyczące działania w przypadku wykrycia naruszenia obowiązujących przepisów dotyczących ochrony prywatności w odniesieniu do przetwarzania danych osobowych, obejmujące przynajmniej obowiązek ustalenia przyczyny i zakresu naruszenia, w celu opisanego jego szkodliwych skutków i podjęcia odpowiednich środków, by uniknąć naruszenia w przyszłości.”

43. Powyższe stanowi przykładowy wykaz środków, które administratorzy danych mogliby wprowadzić w życie, aby wypełnić pierwszą część zasady rozliczalności (*Administrator danych wprowadza odpowiednie i skuteczne środki w celu zapewnienia, że zasady i obowiązki ustanowione w dyrektywie są przestrzegane.*)
44. Niektóre z nich to podstawowe środki, które trzeba będzie wdrożyć w przypadku większości operacji przetwarzania danych. Opracowywanie wewnętrznych strategii i procedur służących wdrażaniu zasad (procedury do rozpatrywania wniosków o udzielenie dostępu, skarg) mogą stanowić przykłady właściwych środków w odniesieniu do niektórych operacji przetwarzania danych. Decyzje o przydatności środków będą musiały być podejmowane po indywidualnym rozpatrzeniu każdego przypadku. Podjęcie takich decyzji należy do administratorów danych, przy uwzględnieniu wytycznych wydanych przez krajowe organy ochrony danych i grupę roboczą art. 29, o ile takie wskazówki są dostępne (zob. poniżej).
45. Z powyższego wynika, że przy określaniu rodzajów środków, które mają zostać wdrożone, nie ma innej drogi niż rozwiązywanie indywidualne. Istotnie, szczególne środki, które należy zastosować, muszą być ustalone zależnie od faktów i okoliczności w każdym indywidualnym przypadku, ze zwróceniem szczególnej uwagi na zagrożenia związane z przetwarzaniem i rodzajami danych. Podejście uniwersalne jedynie zamknęłoby administratorów danych w niedopasowanych strukturach, które ostatecznie zawodzą.
46. W ramach takiego podejścia, administratorzy muszą być w stanie dopasować środki do swoich konkretnych szczególnych okoliczności i poszczególnych operacji przetwarzania danych. W tym kontekście, grupa robocza art. 29 przywołuje kryteria wykorzystane w art. 17 aktualnej dyrektywy⁸ w celu ustalenia rodzaju środków bezpieczeństwa, które mają być zastosowane, mianowicie – zagrożenia wynikające z przetwarzania danych oraz charakter danych. Te dwa czynniki mogłyby być użyte w sposób analogiczny do ustalenia ogólnych rodzajów środków, jakie należy stosować. Ujmując to bardziej precyzyjnie, aspekty takie jak rozmiar operacji przetwarzania danych, zamierzone cele przetwarzania i ilość planowanych przekazów danych mogą określać poziom zagrożenia. Rozważyć należy również rodzaj danych, w tym, czy są to dane szczególnie chronione. W świetle omawianej zasady rozliczalności można by także rozważyć potrzebę nałożenia pewnych obowiązków na osobę przetwarzającą dane lub na programistów, czy producentów z branży TIK (technologie informacyjno-komunikacyjne).
47. Zgodnie z wymienionymi kryteriami administratorzy danych o dużych rozmiarach powinni zasadniczo wdrażać bardziej rygorystycznych środki. W niektórych przypadkach jednak mali lub średni administratorzy danych, w przypadku gdy są zaangażowani w operacje przetwarzania danych obarczone wysokim ryzykiem, takie jak np. operacje przetwarzania danych w odniesieniu do usług elektronicznej opieki zdrowotnej, mogą być także zobowiązani do wprowadzenia rygorystycznych zabezpieczeń. Na przykład: samorząd terytorialny (ratusz),

⁸ „Unwzględniając stan wiedzy w tej dziedzinie oraz koszt realizacji, przyjęte zostaną takie środki, które zapewnią poziom bezpieczeństwa odpowiedni do zagrożeń wynikających z przetwarzania danych oraz charakteru danych objętych ochroną.”

międzynarodowe, małe (internetowe) przedsiębiorstwo, organizacja, dla której przetwarzanie danych jest podstawową działalnością, lub organizacja o historii postępowania niezgodnego z prawem – wszystkie potrzebowałyby własnych, szczególnych środków w celu zapewnienia wiarygodnego i skutecznego systemu zarządzania informacjami. W rezultacie, w przypadkach prostych i podstawowych, takich jak przetwarzanie danych osobowych związanych z zasobami ludzkimi w celu ustanowienia zbiorczego spisu, „obowiązek wykazania”, o którym mowa w ust. 2 przepisu o rozliczalności, mógłby być łatwo spełniony (poprzez np. użyte powiadomienia, opis podstawowych środków bezpieczeństwa, itp.). Jednakże w innych, bardziej skomplikowanych przypadkach, tak jak np. użycie innowacyjnych urządzeń biometrycznych, dopełnienie „obowiązku wykazania” konieczne mogłyby być dalsze wymogi. Administrator może być np. zobowiązany do wykazania, że przeprowadził ocenę skutków w zakresie ochrony prywatności, że personel zaangażowany w przetwarzanie jest przeszkolony i regularnie informowany, itd..

48. Przejrzystość jest integralnym elementem wielu środków dotyczących rozliczalności. Przejrzystość wobec podmiotów danych oraz ogółu ludności zwiększa rozliczalność administratorów danych. Na przykład, większy poziom rozliczalności osiąga się poprzez publikację w Internecie oświadczeń dotyczących ochrony prywatności, poprzez zapewnienie przejrzystości w odniesieniu do wewnętrznych procedur składania skarg i publikację w sprawozdaniach rocznych.

Wytyczne i pewność prawa

49. Podczas gdy potrzeba skalowalności, a zatem elastyczności, przemawia raczej za użyciem otwartego języka, grupa robocza art. 29 ma świadomość, że szeroki przepis umożliwiający elastyczność i skalowalność może także prowadzić do niepewności. Administratorzy mogą także uważać, że przepis nie jest wystarczająco szczegółowy, aby zapewnić pewność prawną. Na przykład może wystąpić niepewność, jeśli chodzi o poziom szczegółowości, którego oczekuje się od strategii i procedur w zakresie prywatności, kiedy i jak wyznaczyć inspektora ds. ochrony danych, kiedy zorganizować sesje szkoleniowe itp. Niepewność ta może także mieć związek z rodzajem weryfikacji, jaki może być niezbędny – wewnętrznie, bądź przez osobę trzecią. Ponadto, administratorzy danych mogą także obawiać się podlegania rozbieżnym i arbitralnym interpretacjom krajowym w odniesieniu do zakresu i charakteru swoich obowiązków.
50. Grupa robocza art. 29 rozumie ten niepokój. Jednak z wymienionych powodów dotyczących potrzeby elastyczności i skalowalności, w samej dyrektywie nie można zawrzeć rozwiązania zapewniającego pewność prawną. Jeśli chodzi o osiągnięcie niezbędnej pewności prawnej, grupa robocza art. 29 uważa, że skutecznym narzędziem, umożliwiającym osiągnięcie większej pewności i wyeliminowanie potencjalnych różnic na poziomie wdrażania mogłoby być zharmonizowanie wytycznych wydanych przez Komicję (np. za pomocą technicznych środków wykonawczych) lub grupę roboczą art. 29.⁹ Grupa robocza

⁹ Przykładem takiego rodzaju wytycznych jest narzędzie samooceny PIPEDA (ang. *Personal Information Protection and Electronic Documents Act*), opublikowane przez Biuro Komisarza ds. Prywatności w Kanadzie (ang. *Office of the Privacy Commissioner of Canada*) w celu pomocy

art. 29 mogłaby także przygotować ogólne wytyczne, zawierające zestaw podstawowych elementów niezbędnych dla standardowego administratora danych, który mógłby być dostosowywany do szczególnych potrzeb każdego administratora danych.

51. Pomocne mogłoby być także opracowanie *wzorcowego programu przestrzegania ochrony danych* (ang. *model data compliance program*), który mógłby być używany przez średnich i dużych administratorów danych jako podstawa, w oparciu o którą mogliby opracowywać swoje poszczególne programy, jak miało to miejsce w przypadku wytycznych opracowanych przez grupę roboczą art. 29 dla BCR¹⁰. Te wzorce powinny być opracowane po dokładnym przeglądzie obecnych praktyk, dostępnych wzorców i konsultacjach ze wszystkimi właściwymi zainteresowanymi stronami. Jest to obszar, który potrzebuje poważnych inwestycji ze strony wszystkich zainteresowanych stron.

Skuteczność środków

52. Identyczne kwestie, jak te omówione powyżej w odniesieniu do środków mających zastosowanie, powstają w kontekście zapewnienia skuteczności środków. W zależności od rodzaju przetwarzania danych, sposób zapewnienia skuteczności może różnić się.
53. Istnieją różne sposoby oceniania przez administratorów danych skuteczności środków (lub jej braku): w przypadku dużych, bardziej złożonych i obarczonych wysokim ryzykiem operacji przetwarzania danych, zwykłymi metodami weryfikacji są wewnętrzne i zewnętrzne audyty. Również sposób, w jaki przeprowadza się audyty, może być różny i może mieć zróżnicowany zakres – od kompleksowych kontroli do kontroli negatywnych (które też mogą przybrać różne formy). W procesie decyzji o tym, jak zapewnić skuteczność środków, grupa robocza art. 29 proponuje użycie tych samych kryteriów co przy podejmowaniu decyzji o środkach, które wynikają z art. 17 dyrektywy 95/46/WE mianowicie, zagrożeń wynikających z przetwarzania danych oraz charakteru danych. Zatem sposób, w jaki administrator powinien zapewnić skuteczność środków, będzie zależał od charakteru danych (chronione bądź nie), ilości przetwarzanych danych i poszczególnych zagrożeń, wynikających z przetwarzania danych. Wytyczne grupy roboczej art. 29 co do środków mogą także obejmować wskazówki dotyczące tego aspektu.

IV.3 Związek z innymi wymogami

Uprzednie zgłoszenia

54. Można by zastanowić się, jaki ewentualny wpływ na uprzednie zgłoszenia będą miały odpowiednie zabezpieczenia na poziomie administratora. Można

średnim i dużym administratorom danych co do opracowania dobrej strategii zarządzania prywatnością i wdrożenia jej. Narzędzie do samooceny jest dostępne na stronie internetowej: http://www.priv.gc.ca/information/pub/ar-vr/pipeda_sa_tool_200807_e.pdf.

¹⁰ Dokument 153 grupy roboczej art. 29 ustanawiający zestaw elementów i zasad zawartych w wiążących przepisach dla przedsiębiorstw (BCR), oraz dokument roboczy 154 ustanawiający ramy struktury wiążących przepisów dla przedsiębiorstw.

przewidzieć, że pewne mechanizmy rozliczalności mogłyby zastąpić lub zmniejszyć wymogi administracyjne obecnego ustawodawstwa dotyczącego ochrony danych, jak to już zasugerowała grupa robocza art. 29 w swojej opinii o przyszłości kwestii prywatności.

Międzynarodowe przesyłanie danych

55. Wiążące zasady dla przedsiębiorstw są przykładem sposobu wdrożenia zasad ochrony danych w oparciu o zasadę rozliczalności. Jest to sposób uznany i przyjęty przez grupę roboczą art. 29 w celu zapewnienia właściwych zabezpieczeń dla przesyłania danych poza Unię Europejską.
56. Jest to obszar, który skorzystałby z dalszej analizy w świetle przeglądu dyrektywy 95/46. W szczególności ważne byłoby rozważenie, czy art. 26 ust. 2 dyrektywy („Państwo Członkowskie może zezwolić na przekazanie [...] danych osobowych [...], jeżeli administrator danych zaleci odpowiednie zabezpieczenia [...]; takie środki zabezpieczające mogą w szczególności wynikać z odpowiednich klauzul umownych.”) w pełni obejmuje wiążące przepisy dla przedsiębiorstw i ostatecznie inne podobne wiążące mechanizmy rozliczalności, jako narzędzia do zapewnienia odpowiednich środków zabezpieczających.
57. W tym kontekście bardzo ważne jest, aby ocenić m. in. mechanizmy używane do wewnętrznego wprowadzenia w życie przez administratorów zasad ochrony danych i obowiązków oraz systemy ich weryfikacji. Jest także istotne, aby przedyskutować mechanizmy służące do udoskonalenia obecnego systemu przesyłania danych przez krajowe organy ochrony danych opartego na autoryzacji.

IV.4 Rola organów ochrony danych

58. Pytanie, na które należy odpowiedzieć, brzmi: czy zasada rozliczalności zaproponowana w niniejszej opinii będzie miała wpływ na uprawnienia organów ochrony danych, w szczególności w obszarze egzekwowania przepisów? Jak poniżej dalej opisano, zasada nie odbiera organom ochrony danych żadnych uprawnień. Wręcz przeciwnie, przyniesie im korzyści.
59. Jeśli chodzi o egzekwowanie, zasada w zaproponowanej formie uznaje uprawnienie organów ochrony danych do wymagania od administratora danych wykazania przestrzegania zasady rozliczalności, a tym samym wspomaga działania organów ukierunkowane na egzekwowanie przepisów. Powyższe zapewnia, że organy pozostają w każdej chwili upoważnione do przeprowadzania działań na rzecz egzekwowania przepisów. Należy wyraźnie stwierdzić, że organy ochrony danych zachowują w każdym razie kompetencję do nadzorowania nie tylko środków podjętych przez administratorów danych, lecz przede wszystkim przestrzegania podstawowych zasad i obowiązków.
60. Ponadto, wprowadzenie w życie zasady rozliczalności zapewni organom ochrony danych użyteczne informacje do monitorowania stopnia przestrzegania przepisów. Istotnie, ze względu na to, że administratorzy danych będą musieli być w stanie

wykazać wobec organów, czy i w jaki sposób wdrożyli środki, organom udostępnione zostaną bardzo ważne informacje dotyczące zgodności z przepisami. Będą one zatem w stanie wykorzystać te informacje w kontekście swoich działań na rzecz egzekwowania przepisów. Ponadto, jeśli takie informacje nie zostaną przedstawione na żądanie, organy ochrony danych będą miały bezpośredni powód do podjęcia działań przeciwko administratorom danych, niezależnie od domniemanego naruszenia pozostałych podstawowych zasad ochrony danych.

61. Zasada powinna także służyć organom ochrony danych pozwalając im na bardziej selektywne i strategiczne działanie i umożliwiając zainwestowanie swoich zasobów tak, aby osiągnąć największy możliwy stopień przestrzegania przepisów.
62. Grupa robocza art. 29 zauważa, że zasada rozliczalności może przyczynić się do rozwoju prawnej i technicznej ekspertyzy w dziedzinie wdrażania wymogów ochrony danych. Osoby posiadające dużą znajomość technicznych i prawnych aspektów w dziedzinie ochrony danych, z umiejętnością komunikacji, szkolenia personelu, ustanawiania i wdrażania strategii oraz przeprowadzania audytu będą w tym obszarze niezbędne. Taka ekspertyza będzie niezbędna zarówno wewnątrz przedsiębiorstw, jak i w przypadku usług zleczanych firmom zewnętrznym. Zmiana ta odegra istotną rolę w zagwarantowaniu, że administratorzy danych są w stanie dopełnić swoich obowiązków, w tym, w razie konieczności, przeprowadzać wewnętrzne i zewnętrzne/wewnętrzne audyty. Jednocześnie taki rozwój sytuacji będzie korzystny dla organów ochrony danych, ponieważ system będzie przyczyniał się do ogólnego przestrzegania przepisów, organy będą miały do swojej dyspozycji więcej rzetelnych informacji o wewnętrznych praktykach przedsiębiorstw, a powstanie grupy wykwalifikowanych specjalistów posiadających umiejętności w dziedzinie ochrony danych z pewnością ułatwi codzienną współpracę tych organów z administratorami danych.
63. Podsumowując, można stwierdzić, że działania organów ochrony danych są bardziej skoncentrowane na roli *ex post*, niż *ex ante*. Ze względu na to, że w ramach rozliczalności kładzie się nacisk na osiągnięcie pewnych rezultatów, np. w zakresie dobrego zarządzania ochroną danych, można stwierdzić, że jest ona ukierunkowana na wyniki; przy czym nacisk kładzie się na środki podejmowane *ex post* (tj. po rozpoczęciu przetwarzania danych).

IV.5 Sankcje

64. Zaproponowany system może funkcjonować jedynie, gdy organom ochrony danych przyzna się kompetencje do skutecznego nakładania sankcji. Potrzeba zastosowania skutecznych sankcji zachodzi w szczególności, gdy i o ile administratorzy danych nie dopełniają swoich obowiązków wynikających z zasady rozliczalności. Na przykład należy nałożyć karę, gdy administrator danych nie respektuje oświadczeń, które poczynił w wiążących strategiach wewnętrznych. To poszerza dodatkowo faktyczne naruszenie podstawowych zasad ochrony danych.
65. Ponadto, grupa robocza art. 29 uważa, że uprawnienia krajowych organów ochrony danych powinny obejmować możliwość wprowadzenia szczegółowych instrukcji dla administratorów danych w odniesieniu do ich systemów zgodności.

IV.6 Opracowywanie systemów certyfikacji

66. W dłuższym okresie czasu, przepis dotyczący rozliczalności wsparłby rozwój programów certyfikacji lub certyfikatów bezpieczeństwa. Takie programy mogłyby przyczyniać się do udowodnienia, że administrator danych wypełnił przepis, ponieważ określił i wdrożył odpowiednie środki, które były okresowo kontrolowane. Taki rozwój mogą wspierać różne czynniki:
67. Ogólnie rzecz biorąc, można oczekiwać, że aby odróżnić się, usługodawcy w zakresie ochrony danych, przeprowadzania oceny skutków w zakresie ochrony prywatności, przeprowadzania audytu, będą prawdopodobnie coraz częściej proponować certyfikaty bezpieczeństwa w celu wyróżnienia się na rynku i zdobycia przewagi konkurencyjnej. Administratorzy danych mogą podjąć decyzję o certyfikacji przez wiarygodnych usługodawców. Ponieważ stanie się wiadome, że niektóre certyfikaty bezpieczeństwa wiążą się z rygorystycznymi kontrolami, prawdopodobne jest, że administratorzy danych będą je preferować, ponieważ dawałyby one większą pewność w kwestii zgodności, oprócz oferowania przewagi konkurencyjnej.
68. Wykorzystanie BCR jako podstawy prawnej dla międzynarodowego przesyłania danych wymagałoby wykazania przez administratorów danych, że wprowadzili oni w życie odpowiednie zabezpieczenia, w związku z czym organy ochrony danych mogłyby autoryzować przesyłanie. Jest to obszar, w którym usługi certyfikacji byłyby pomocne. Takie usługi analizowałyby gwarancje zapewnione przez administratora danych i, jeśli możliwe, wydawałyby właściwy certyfikat bezpieczeństwa. Organ ochrony danych mógłby korzystać z certyfikacji zapewnionych przez dany program certyfikacyjny w swoich analizach BCR dotyczących tego, czy administrator danych zapewnił wystarczające zabezpieczenie dla celów międzynarodowego przesyłania danych. To z kolei przyczyniłoby się do usprawnienia procesu autoryzacji w międzynarodowym przesyłaniu danych.

IV.7 Uregulowanie dotyczące systemów certyfikacji

69. Z tych samych powodów, które przemawiają za rozwojem usług certyfikacyjnych, konieczne jest uregulowanie tych usług. Istotnie, jeśli takie usługi mają zapewnić rzetelne dowody na zgodność z zasadami ochrony danych (organom ochrony danych, administratorom i ogółowi konsumentów) i płynnie funkcjonować na rynku wewnętrznym, niezbędne wydaje się ustanowienie zasad określających wymogi dotyczące świadczenia takich usług. Organy ochrony danych powinny odgrywać główną rolę przy opracowaniu tych zasad (wskazówki, wzorce, itp.) i powinny być w stanie egzekwować ich stosowanie. Oznacza to również, że w tym celu organy powinny posiadać wystarczające zasoby. Ponadto, organy ochrony danych powinny brać udział w akredytowaniu jednostek certyfikujących. Może być to szczególnie ważne w obszarze międzynarodowego przesyłania danych. Ponieważ jakoś takich usług i potrzeba, aby działały na rynku wewnętrznym są kryterium kluczowym, ustawodawca musi stworzyć warunki umożliwiające osiągnięcie takiej jakości. Pozostawienie tej kwestii rynkowi nie wydaje się możliwe. Doświadczenie w innych obszarach, takich jak certyfikacja towarów,

wskazuje na tendencję obniżania poziomu. Konkurencja pomiędzy dostawcami usług może prowadzić do obniżenia cen i także do pewnej elastyczności, lub rozluźnienia procedur. Podsumowując, bez względu na to, czy operacje mają charakter transgraniczny, czy też nie, przepisy wydają się konieczne, aby zapewnić wysoką jakość usług i równe szanse.

70. Grupa robocza art. 29 zauważa, że istniejące ustawodawstwo dotyczące akredytacji¹¹ może być stosowane w obszarze usług certyfikacyjnych w dziedzinie ochrony danych. Takie ustawodawstwo już zapewnia niezbędne struktury ustanawiające zasady dotyczące organizacji i działania jednostek akredytujących. Zasady te mają zastosowanie do dobrowolnych akredytacji, a w szczególnych przypadkach także do obowiązkowych akredytacji.
71. Ten rodzaj usług oczywiście przyczyniałby się również do harmonizacji podstawowych standardów, stanowiących podstawę testowania podmiotów. Wspomniane wytyczne (opracowane przez grupę roboczą art. 29 lub Komisję) ustanawiające wzorcowe programy przestrzegania ochrony danych byłyby niezwykle cenne.

V. WNIOSKI

72. Rozwój nowych technologii oraz postępujący proces globalizacji w gospodarce i społeczeństwie doprowadziły do rozprzestrzeniania się danych osobowych, które są gromadzone, sortowane, przesyłane lub w inny sposób przechowywane. Zatem mnożą się zagrożenia, na które wystawione są takie dane.
73. Grupa robocza art. 29 jest przekonana, że wzrost zarówno zagrożeń dla danych osobowych, jak i wzrost wartości tych danych same w sobie przemawiają za potrzebą wzmocnienia roli i odpowiedzialności administratorów danych. Ramy prawne, które stosują się do tych nowych realiów, muszą obejmować niezbędne narzędzia, aby zachęcić administratorów danych do stosowania w praktyce właściwych i skutecznych środków, które prowadzących do osiągnięcia zamierzonych celów w odniesieniu do zasad ochrony danych. Przykładami takich środków są procedury zapewniające identyfikację wszystkich operacji przetwarzania danych, odpowiedzi na wnioski o udzielenie dostępu, przydzielenie zasobów, w tym wyznaczenie osób, które są odpowiedzialne za organizację przestrzegania przepisów w zakresie ochrony danych.
74. Aby zachęcić do ochrony danych w praktyce, grupa robocza art. 29 sugeruje przede wszystkim zawarcie w propozycjach zmieniających dyrektywę o ochronie danych nowy przepis, który zobowiązywałby administratorów danych do wdrożenia właściwych i skutecznych środków w celu zapewnienia, że zasady i obowiązki wynikające z dyrektywy o ochronie danych są stosowane i wykazywania tego na żądanie organów. Te środki powinny przyczynić się do przestrzegania zasad i obowiązków w zakresie ochrony danych, a jednocześnie zminimalizować zagrożenie nieuprawnionego dostępu, niewłaściwego użycia

¹¹ Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie (EWG) nr 339/93.

bądź utraty itp. Obowiązek wykazania na żądanie wprowadzenia niezbędnych środków powinien stanowić użyteczne narzędzie dla organów ochrony danych do egzekwowania przepisów.

75. Obowiązek wdrożenia tych środków powinien mieć zastosowanie wobec administratorów danych wszystkich sektorów (publicznego i prywatnego) i powinien być skalowalny w taki sposób, aby rodzaj środków odpowiadał zagrożeniom wynikającym z przetwarzania danych i charakteru danych.

Sporządzono w Brukseli dnia 13 lipca 2010 r.

*W imieniu grupy roboczej
Przewodniczący
Jacob KOHNSTAMM*