GRUPA ROBOCZA DS. OCHRONY DANYCH POWOŁANA NA MOCY ART. 29

00264/10/PL
WP 169

Opinia 1/2010 w sprawie pojęć „administrator danych” i „przetwarzający”

przyjęta w dniu 16 lutego 2010 r.

SPIS TREŚCI

Streszczenie

Pojęcie administratora danych i jego interakcja z pojęciem przetwarzającego odgrywają zasadniczą rolę w stosowaniu dyrektywy 95/46/WE, ponieważ określają, kto odpowiada za zgodność z zasadami ochrony danych, w jaki sposób osoby, których dane dotyczą, mogą wykonywać swoje prawa, jakie prawo krajowe ma zastosowanie i jak skutecznie mogą działać organy ochrony danych.

Zróżnicowanie organizacyjne sektora publicznego i prywatnego, rozwój technologii informacyjno-komunikacyjnych (TIK) oraz globalizacja przetwarzania danych zwiększają złożoność sposobu przetwarzania danych osobowych i wiążą się z koniecznością wyjaśnienia omawianych pojęć w celu zapewnienia skutecznego stosowania i zgodności w praktyce.

Pojęcie administratora danych jest autonomiczne w tym sensie, że należy je interpretować głównie według wspólnotowych przepisów o ochronie danych, i funkcjonalne w tym sensie, że ma na celu przydzielanie obowiązków tam, gdzie występuje faktyczny wpływ, a zatem opiera się raczej na analizie okoliczności faktycznych niż na analizie formalnej.

Definicja zamieszczona w dyrektywie składa się z trzech głównych modułów:
- aspektów o charakterze osobistym („osoba fizyczna lub prawna, władza publiczna, agencja lub inny organ”);
- możliwości kontroli pluralistycznej („który samodzielnie lub wspólnie z innymi podmiotami”) oraz
- zasadniczych elementów odróżniających administratora danych od innych podmiotów („określa cele i sposoby przetwarzania danych”).

Analiza tych elementów składowych prowadzi do szeregu wniosków, które podsumowano w pkt IV opinii.

W niniejszej opinii przeprowadzono również analizę pojęcia przetwarzającego. Jego istnienie zależy od decyzji podjętej przez administratora danych, który może podjąć decyzję o przetwarzaniu danych w swojej organizacji lub o przekazaniu całości bądź części działań związanych z przetwarzaniem organizacji zewnętrznej. Podmiot może być przetwarzającym, jeżeli spełnia dwa podstawowe warunki: po pierwsze, jest odrębną osobą prawną w stosunku do administratora danych, po drugie, przetwarza dane osobowe w jego imieniu.

Grupa robocza dostrzega trudności w stosowaniu definicji użytych do celów dyrektywy w złożonych okolicznościach, w których można przewidzieć wiele scenariuszy samodzielnego lub wspólnego funkcjonowania administratorów danych i przetwarzających o różnym stopniu autonomii i odpowiedzialności.

W analizie grupa robocza podkreśliła potrzebę powierzenia odpowiedzialności w taki sposób, aby zapewnić w praktyce wystarczającą zgodność z przepisami dotyczącymi ochrony danych. Nie znalazła jednak powodów, aby przypuszczać, że obecne rozróżnienie pomiędzy administratorami danych i przetwarzającymi nie będzie już w tej perspektywie odpowiednie i użyteczne.

Grupa robocza ma zatem nadzieję, że przedstawione w niniejszej opinii wyjaśnienia, zilustrowane konkretnymi przykładami zaczerpniętymi z codziennych doświadczeń organów ochrony danych, pomogą w interpretacji tych podstawowych definicji zawartych w dyrektywie.

Grupa Robocza ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych

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

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

uwzględniając swój regulamin,

przyjmuje następującą opinię:

I. Wprowadzenie

Pojęcie administratora danych i jego interakcja z pojęciem przetwarzającego odgrywają zasadniczą rolę w stosowaniu dyrektywy 95/46/WE, ponieważ określają, kto odpowiada za zgodność z zasadami ochrony danych, i w jaki sposób osoby, których dane dotyczą, mogą w praktyce wykonywać swoje prawa. Pojęcie administratora danych ma także zasadnicze znaczenie przy określaniu właściwego prawa krajowego i skutecznym wykonywaniu zadań nadzorczych powierzonych organom ochrony danych.

W związku z tym niezwykle istotne jest, aby dokładne znaczenie tych pojęć i kryteria ich poprawnego stosowania były wystarczająco jasne i stosowane przez wszystkich, którzy w państwach członkowskich odgrywają rolę w wykonywaniu dyrektywy, a także w stosowaniu, ocenie i przestrzeganiu nadających jej skuteczność przepisów krajowych.

Pewne oznaki wskazują na brak jasności przynajmniej w odniesieniu do niektórych aspektów tych pojęć, a wśród praktyków w różnych państwach członkowskich występują rozbieżne opinie, które mogą prowadzić do różnej interpretacji tych samych zasad i definicji wprowadzonych do celów harmonizacji na szczeblu europejskim. Dlatego grupa robocza art. 29 postanowiła – w ramach strategicznego programu prac na lata 2008–2009 – poświęcić szczególną uwagę opracowaniu dokumentu określającego wspólne podejście do tych kwestii.

Grupa robocza uznaje, że konkretne stosowanie pojęć administratora danych i przetwarzającego dane staje się coraz bardziej złożone. Wynika to głównie z rosnącej złożoności środowiska, w jakim stosuje się te pojęcia, oraz w szczególności ze względu na coraz powszechniejszą tendencję, zarówno w sektorze prywatnym jak i publicznym, do różnicowania organizacyjnego, w połączeniu z rozwojem TIK i globalizacją, co może prowadzić do pojawiania się nowych i trudnych kwestii oraz skutkować niekiedy niższym poziomem ochrony zapewnianej osobom, których dane dotyczą.

Chociaż przepisy dyrektywy sformułowano w sposób neutralny technologicznie i dotychczas bronią się one skutecznie przed zmieniającym się kontekstem, ten złożony charakter może rzeczywiście prowadzić do braku pewności w odniesieniu do powierzania odpowiedzialności i zakresu właściwego prawa krajowego. Brak pewności może mieć negatywny wpływ na zgodność z przepisami dotyczącymi ochrony danych w kluczowych obszarach oraz na skuteczność przepisów o ochronie danych jako całości. Grupa robocza zajęła się już niektórymi z tych spraw w związku z konkretnymi

pytaniami[1], ale w chwili obecnej uważa za niezbędne przedstawienie bardziej rozbudowanych wytycznych i konkretnych wskazówek w celu zapewnienia spójnego i zharmonizowanego podejścia.

Grupa robocza postanowiła zatem przekazać w niniejszej opinii – podobnie jak uczyniła to w Opinii w sprawie pojęcia danych osobowych[2] – pewne wyjaśnienia i konkretne przykłady[3] odnoszące się do pojęć administratora danych i przetwarzającego dane.

II. Uwagi ogólne i kwestie dotyczące polityki

Dyrektywa wyraźnie odwołuje się w kilku przepisach do pojęcia administratora danych. Definicje „administratora danych" i „przetwarzającego" w art. 2 lit. d) i e) dyrektywy 95/46/WE (zwanej dalej „dyrektywą") mają następujące brzmienie:

> *„administrator danych" oznacza osobę fizyczną lub prawną, władzę publiczną, agencję lub inny organ, który samodzielnie lub wspólnie z innymi podmiotami określa cele i sposoby przetwarzania danych; jeżeli cele i sposoby przetwarzania danych są określane w przepisach ustawowych i wykonawczych lub przepisach wspólnotowych, administrator danych może być powoływany lub kryteria jego powołania mogą być ustalane przez ustawodawstwo krajowe lub wspólnotowe;*
>
> *„przetwarzający" oznacza osobę fizyczną lub prawną, władzę publiczną, agencję lub inny organ przetwarzający dane osobowe w imieniu administratora danych*.

Definicje te sformułowano na początku lat 90. XX wieku podczas negocjacji w sprawie projektu wniosku dotyczącego dyrektywy, a pojęcie „administratora danych" zaczerpnięto zasadniczo z konwencji nr 108 Rady Europy zawartej w 1981 r. Podczas negocjacji wprowadzono kilka ważnych zmian.

Po pierwsze „administratora zbioru danych" z konwencji nr 108 zastąpiono „administratorem danych" w odniesieniu do „przetwarzania danych osobowych". Jest to szerokie pojęcie zdefiniowane w art. 2 lit. b) dyrektywy jako „każda operacja lub zestaw operacji dokonywanych na danych osobowych przy pomocy środków zautomatyzowanych lub innych, jak np. gromadzenie, rejestracja, porządkowanie, przechowywanie, adaptacja lub modyfikacja, odzyskiwanie, konsultowanie, wykorzystywanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, układanie lub kompilowanie, blokowanie, usuwanie lub niszczenie". Pojęcia „administratora danych" nie stosowano już zatem w odniesieniu do przedmiotu („zbiór danych"), ale w odniesieniu do działań odzwierciedlających cykl życia informacji od jej pozyskania po zniszczenie, na które należy spojrzeć zarówno szczegółowo, jak i całościowo („operacja lub zestaw operacji"). Chociaż w wielu przypadkach wyniki mogły być takie same, pojęciu nadano szersze i bardziej dynamiczne znaczenie i zakres.

---

1 Zob. np. Opinia 10/2006 w sprawie przetwarzania danych osobowych przez Stowarzyszenie Międzynarodowej Teletransmisji Danych Finansowych (Society for Worldwide Interbank Financial Communication, SWIFT) przyjęta w dniu 22 listopada 2006 r. (WP 128) i niedawna Opinia 5/2009 w sprawie portali społecznościowych przyjęta w dniu 12 czerwca 2009 r. (WP 163).

2 Opinia 4/2007 w sprawie pojęcia danych osobowych przyjęta w dniu 20 czerwca 2007 r. (WP 136)

3 Przykłady te oparto na aktualnej praktyce krajowej lub europejskiej; w celu zapewnienia lepszego zrozumienia mogły one zostać zmienione lub przeredagowane.

Inne zmiany obejmowały wprowadzenie możliwości „kontroli pluralistycznej” („samodzielnie lub wspólnie z innymi podmiotami”), wymogu, zgodnie z którym administrator danych „określa cele i sposoby przetwarzania danych”, i koncepcji, zgodnie z którą takiego określenia można dokonać poprzez prawodawstwo krajowe lub wspólnotowe bądź w inny sposób. W dyrektywie wprowadzono także pojęcie przetwarzającego, którego nie wymieniono w konwencji nr 108. Te i inne zmiany zostaną przeanalizowane bardziej szczegółowo w niniejszej opinii.

II.1. Rola pojęć

O ile w konwencji nr 108 pojęcie administratora (zbioru danych) odgrywa bardzo ograniczoną rolę[4], w dyrektywie sytuacja przedstawia się zupełnie inaczej. Art. 6 ust. 2 wyraźnie stanowi, że „na administratorze danych spoczywa obowiązek zapewnienia przestrzegania przepisów ust. 1”. Odnosi się to do głównych zasad dotyczących jakości danych, w tym do zasady z art. 6 ust. 1 lit. a), zgodnie z którą dane osobowe są „przetwarzane rzetelnie i legalnie”. W rzeczywistości oznacza to, że wszystkie przepisy określające warunki legalnego przetwarzania danych są skierowane zasadniczo do administratora danych, nawet jeżeli nie zawsze wyrażono to w jasny sposób.

Ponadto przepisy dotyczące praw osoby, której dane dotyczą, do informacji, wglądu, sprostowania, usuwania i blokowania oraz do sprzeciwu wobec przetwarzania danych osobowych (art. 10–12 i 14) sformułowano w sposób, który nakłada obowiązki na administratora danych. Administrator danych odgrywa także kluczową rolę w przepisach dotyczących powiadomienia i kontroli wstępnej (art. 18-21). Nie powinno wreszcie dziwić, że administrator danych odpowiada zasadniczo także za wszelkie szkody poniesione wskutek niezgodnego z prawem przetwarzania (art. 23).

Oznacza to, że w przypadku pojęcia administratora danych podstawową i najważniejszą rolą jest określenie, kto odpowiada za zgodność z zasadami ochrony danych i w jaki sposób osoby, których dane dotyczą, mogą w praktyce wykonywać swoje prawa[5]. Innymi słowy: powierzenie odpowiedzialności.

Dotyka to samej istoty dyrektywy, której pierwszym celem jest „ochrona osób fizycznych w zakresie przetwarzania danych osobowych”. Cel ten można zrealizować i skutecznie zastosować w praktyce wyłącznie, jeżeli osoby odpowiedzialne za przetwarzanie danych będą dostatecznie stymulowane instrumentami prawnymi i innymi instrumentami do podejmowania wszelkich środków niezbędnych w celu zapewnienia tej ochrony w praktyce. Potwierdza to art. 17 ust. 1 dyrektywy, zgodnie z którym administrator danych „wprowadza odpowiednie środki techniczne i organizacyjne w celu ochrony danych osobowych przed przypadkowym lub nielegalnym zniszczeniem lub przypadkową utratą, zmianą, niedozwolonym ujawnieniem lub dostępem, szczególnie

[4] Nie stosuje się go w żadnym z merytorycznych przepisów, z wyjątkiem art. 8 lit. a) w odniesieniu do prawa do bycia informowanym (zasada przejrzystości). Administrator danych, jako strona odpowiedzialna, jest widoczny jedynie w niektórych częściach uzasadnienia.

[5] Zob. także motyw 25 dyrektywy 95/46/WE: „Zasady ochrony muszą znajdować odzwierciedlenie, z jednej strony w obowiązkach nałożonych na osoby, władze publiczne, przedsiębiorstwa, agencje i inne organy odpowiedzialne za przetwarzanie danych, zwłaszcza w zakresie jakości danych, bezpieczeństwa technicznego, zawiadamiania organu nadzorczego oraz okoliczności, w których może odbywać się przetwarzanie danych, jak również, z drugiej strony, w prawie osób, których dane są przedmiotem przetwarzania, do uzyskania informacji, że takie przetwarzanie danych ma miejsce, do konsultowania danych, żądania poprawek lub nawet sprzeciwu wobec przetwarzania danych w niektórych przypadkach.”.

wówczas gdy przetwarzanie danych obejmuje transmisję danych w sieci, jak również przed wszelkimi innymi nielegalnymi formami przetwarzania".

Instrumenty wzbudzania odpowiedzialności mogą mieć charakter proaktywny i reaktywny. W pierwszym przypadku mają zapewnić skuteczne wprowadzanie w życie środków ochrony danych i dostatecznych środków odpowiedzialności w stosunku do administratorów danych. W drugim przypadku mogą obejmować odpowiedzialność cywilną i sankcje mające na celu zapewnienie rekompensaty z tytułu wszystkich stosownych szkód i podjęcia odpowiednich środków zmierzających do naprawy błędów lub nieprawidłowości.

Pojęcie administratora danych jest także zasadniczym elementem przy określaniu, które prawo krajowe ma zastosowanie do operacji przetwarzania lub zestawu operacji przetwarzania. Główna zasada prawa właściwego zgodnie z art. 4 ust. 1 lit. a) dyrektywy stanowi, że każde państwo członkowskie stosuje przepisy prawa krajowego w odniesieniu do „przetwarzania danych osobowych „wówczas, gdy przetwarzanie danych odbywa się w kontekście prowadzenia przez administratora danych działalności gospodarczej na terytorium państwa członkowskiego". Dalsza część przepisu stanowi, że: „jeżeli ten sam administrator danych prowadzi działalność gospodarczą na terytorium kilku państw członkowskich, musi on podjąć niezbędne działania, aby zapewnić, że każde z tych przedsiębiorstw wywiązuje się z obowiązków przewidzianych w odpowiednich przepisach prawa krajowego". Oznacza to, że przedsiębiorstwo (przedsiębiorstwa) administratora danych ma (mają) znaczenie rozstrzygające w kwestii właściwego prawa krajowego oraz ewentualnie w kwestii kilku różnych właściwych praw krajowych i sposobu, w jaki te prawa są ze sobą powiązane[6].

Należy również zauważyć, że pojęcie administratora danych pojawia się w wielu różnych przepisach dyrektywy jako element ich zakresu lub szczególnego warunku stosowanego w ramach tych przepisów, np. art. 7 stanowi, że dane osobowe mogą być przetwarzane tylko wówczas gdy: „c) przetwarzanie danych jest konieczne dla wykonania zobowiązania prawnego, któremu administrator danych podlega, e) przetwarzanie danych jest konieczne dla realizacji zadania wykonywanego w interesie publicznym lub dla wykonywania władzy publicznej przekazanej administratorowi danych lub osobie trzeciej, przed którą ujawnia się dane lub f) przetwarzanie danych jest konieczne dla potrzeb wynikających z uzasadnionych interesów administratora danych lub osoby trzeciej, lub osobom, którym dane są ujawniane, z wyjątkiem sytuacji, kiedy interesy takie podporządkowane są …". Tożsamość administratora danych jest także ważnym elementem informacji dla osoby, której dane dotyczą, wymaganym na mocy art. 10 i 11.

Pojęcie „przetwarzającego" odgrywa ważną rolę w kontekście poufności i bezpieczeństwa przetwarzania danych (art. 16–17), ponieważ służy określaniu obowiązków osób, które są ściślej zaangażowane w przetwarzanie danych osobowych pod bezpośrednim zwierzchnictwem administratora danych lub w jego imieniu. Rozróżnienie między „administratorem danych" a „przetwarzającym" służy głównie rozróżnieniu między zaangażowanymi podmiotami odpowiedzialnymi jako administrator (administratorzy) danych a podmiotami, które jedynie działają w ich imieniu. Po raz

[6] Grupa robocza zamierza przyjąć w 2010 r. odrębną opinię na temat „prawa właściwego". W przypadku przetwarzania danych osobowych przez instytucje i organy wspólnotowe ocena administrowania danymi może mieć również znaczenie dla ewentualnego stosowania rozporządzenia (WE) nr 45/2001 lub innych właściwych instrumentów prawnych UE.

kolejny jest to głównie kwestia sposobu powierzania odpowiedzialności. Mogą z tego wynikać inne skutki pod względem prawa właściwego lub pod innym względem.

W przypadku przetwarzającego ma to jednak jeszcze jeden skutek – zarówno w odniesieniu do administratora danych, jak i do przetwarzającego – tj., że na podstawie art. 17 dyrektywy prawem właściwym dla bezpieczeństwa przetwarzania danych jest prawo krajowe państwa członkowskiego, w którym przetwarzający prowadzi działalność gospodarczą.[7]

Zgodnie z definicją zawartą w art. 2 lit. f), „»osoba trzecia« oznacza osobę fizyczną lub prawną, władzę publiczną, agencję lub inny organ niebędący osobą, której dane dotyczą, ani administratorem danych, ani przetwarzającym lub jedną z osób, które pod bezpośrednim zwierzchnictwem administratora danych lub przetwarzającego upoważnione są do przetwarzania danych". Administratora danych i przetwarzającego oraz ich personel uważa się zatem za „wąskie grono przetwarzania danych" i nie objęci są oni szczególnymi przepisami dotyczącymi osób trzecich.

II.2. Odpowiedni kontekst

Zmieniające się okoliczności w przedmiotowym środowisku sprawiły, że kwestie te stały się pilniejsze i bardziej złożone niż wcześniej. W chwili podpisywania konwencji nr 108, a także w znacznym stopniu w czasie przyjmowania dyrektywy 95/46/WE, kontekst przetwarzania danych był nadal względnie jasny i przystępny, jednak obecnie sytuacja uległa zmianie.

Jest to w pierwszej kolejności spowodowane coraz bardziej powszechną tendencją do zróżnicowania organizacyjnego w najbardziej znaczących sektorach. W sektorze prywatnym podział ryzyka finansowego i ryzyka o innym charakterze doprowadził do ciągłej dywersyfikacji przedsiębiorstw, którą dodatkowo jeszcze nasilają połączenia i przejęcia. W sektorze publicznym podobne zróżnicowanie odbywa się w kontekście decentralizacji lub rozdzielania departamentów odpowiedzialnych za poszczególne dziedziny polityki i agencji wykonawczych. W obydwu sektorach coraz większy nacisk kładzie się na rozwój łańcuchów dostaw lub świadczenie usług w organizacjach i stosowanie podwykonawstwa lub outsourcingu usług w celu skorzystania ze specjalizacji i ewentualnych korzyści skali. W rezultacie następuje wzrost w zakresie różnych usług oferowanych przez usługodawców, którzy nie zawsze uważają się za odpowiedzialnych i rozliczalnych. Wskutek wyborów organizacyjnych dokonywanych przez przedsiębiorstwa (a także decyzji wykonawców i podwykonawców) przedmiotowe bazy danych mogą być umiejscowione w co najmniej jednym państwie Unii Europejskiej lub poza jej granicami.

Rozwój technologii informacyjno-komunikacyjnych („TIK") znacznie ułatwił te zmiany organizacyjne, a także przyniósł ze sobą kilka własnych. Obowiązki na różnych szczeblach – wynikające często ze zróżnicowania organizacyjnego – wymagają zwykle szerokiego stosowania TIK, a także pobudzają ich stosowanie. Opracowywanie i wdrażanie produktów i usług TIK prowadzi także do powstawania nowych odrębnych ról i obowiązków, których interakcje z istniejącymi lub rozwijającymi się obowiązkami w organizacjach klientów nie zawsze są jasne. W związku z tym ważne jest, aby mieć

[7] Zob. art. 17 ust. 3 tiret drugie: „obowiązki (...) określone przez ustawodawstwo państwa członkowskiego, w którym podmiot przetwarzający prowadzi działalność gospodarczą, dotyczą również podmiotu przetwarzającego".

świadomość istotnych różnic i w razie potrzeby wyjaśniać kwestie obowiązków. Z wprowadzeniem mikrotechnologii – takiej jak mikroprocesory RFID stosowane w produktach konsumenckich – wiążą się podobne kwestie przenoszenia obowiązków. Z drugiej strony występują nowe i trudne kwestie związane ze stosowaniem obliczeń rozproszonych, w szczególności tzw. przetwarzania w chmurze („cloud computing") i przetwarzania sieciowego („grid")[8].

Kolejnym czynnikiem komplikującym sytuację jest globalizacja. Gdy zróżnicowanie organizacyjne i opracowywanie TIK podlega wielu jurysdykcjom, co często ma miejsce w odniesieniu do internetu, w sposób nieunikniony pojawiają się kwestie prawa właściwego, nie tylko w obrębie UE lub EOG, ale także w odniesieniu do państw trzecich. Ilustrację tej sytuacji można znaleźć kontekście antydopingowym, w którym Światowa Agencja Antydopingowa (WADA) z siedzibą w Szwajcarii, prowadzi bazę danych zawierającą informacje na temat sportowców (ADAMS), zarządzaną z Kanady we współpracy z krajowymi organizacjami antydopingowymi z całego świata. Grupa robocza art. 29 wskazała podział obowiązków i przydział administrowania danymi jako kwestie, które sprawiają szczególne trudności[9].

Oznacza to, że podstawowe kwestie zawarte w tej opinii mają pierwszorzędne znaczenie praktyczne i mogą mieć poważne konsekwencje.

II.3. Niektóre kluczowe kwestie

W świetle celów dyrektywy najważniejsze jest zapewnienie wyraźnego określenia odpowiedzialności za przetwarzanie danych i jej skutecznego stosowania.

Jeżeli wymagania wobec poszczególnych osób nie są dostatecznie jasne (np. nikt nie ponosi odpowiedzialności lub jest wielu ewentualnych administratorów danych), istnieje oczywiste ryzyko, że zbyt mało lub nic nie zostanie zrobione i że przepisy prawne pozostaną nieskuteczne. Niejednoznaczności w interpretowaniu mogą również doprowadzić do konkurujących żądań i innych kontrowersji; w takim przypadku pozytywne skutki będą mniejsze niż oczekiwano bądź ograniczą je lub przeważą nad nimi nieprzewidziane skutki negatywne.

We wszystkich takich przypadkach głównym wyzwaniem jest zapewnienie wystarczającej jasności umożliwiającej i gwarantującej skuteczne stosowanie i zgodność w praktyce. W przypadku wątpliwości preferowanym wariantem może być rozwiązanie, które będzie najlepiej promowało takie efekty.

Jednak te same kryteria, które zapewniają wystarczającą jasność, mogą także prowadzić do dodatkowych komplikacji i niepożądanych konsekwencji. Przykładowo zróżnicowanie administrowania danymi zgodne z rzeczywistością organizacyjną może

---

[8] „Przetwarzanie w chmurze" to rodzaj przetwarzania, w którym skalowalne i elastyczne zdolności IT oferuje się w formie usługi wielu klientom przy zastosowaniu technologii internetowych. Typowe usługi w chmurach obliczeniowych udostępniają popularne aplikacje biznesowe on-line, do których dostęp uzyskuje się z przeglądarki internetowej, natomiast oprogramowanie i dane są przechowywane na serwerach. W związku z tym chmura nie jest wyspowym, ale globalnym łącznikiem między informacjami ze świata i użytkownikami. W odniesieniu do przetwarzania sieciowego zob. przykład 19 poniżej.

[9] Opinia 3/2008 z dnia 1 sierpnia 2008 r. dotycząca projektu międzynarodowego standardu ochrony prywatności dla Światowego kodeksu antydopingowego, WP156.

prowadzić do złożoności właściwego prawa krajowego w przypadku różnych jurysdykcji.

Analiza powinna zatem wnikliwie oceniać różnicę między konsekwencjami akceptowalnymi w ramach obecnych zasad a ewentualną potrzebą dostosowania aktualnych zasad w celu zapewnienia stałej skuteczności i uniknięcia niewłaściwych konsekwencji w zmieniających się okolicznościach.

Oznacza to, że niniejsza analiza ma duże znaczenie strategiczne i należy ją stosować z ostrożnością oraz pełną świadomością ewentualnych wzajemnych powiązań między różnymi sprawami.

III. Analiza definicji

III.1. Definicja administratora danych

Definicja administratora danych zamieszczona w dyrektywie składa się z trzech głównych modułów, które dla celów niniejszej opinii zostaną poddane odrębnej analizie. Są to następujące moduły:

- „osoba fizyczna lub prawna, władza publiczna, agencja lub inny organ"
- „który samodzielnie lub wspólnie z innymi podmiotami"
- „określa cele i sposoby przetwarzania danych".

Pierwszy moduł odnosi się do personalnego aspektu definicji. Trzeci moduł obejmuje podstawowe elementy odróżniające administratora danych od innych podmiotów, natomiast drugi moduł uwzględnia możliwość istnienia „kontroli pluralistycznej". Omawiane moduły są ściśle ze sobą powiązane, jednak ze względu na metodologię przyjętą w niniejszej opinii każda z tych pozycji zostanie omówiona oddzielnie.

Ze względów praktycznych lepiej jest rozpocząć od *pierwszego elementu* trzeciego modułu – tj. znaczenia słowa „określa" – następnie omówić pozostałe jego elementy, a dopiero później przejść do pierwszego i drugiego modułu.

III.1.a) Element wstępny: „określa"

Jak wspomniano powyżej pojęcie administratora danych odgrywało niewielką rolę w konwencji nr 108. Zgodnie z art. 2 konwencji „administratora zbioru danych" zdefiniowano jako organ „właściwy … do określenia". W konwencji podkreślono potrzebę istnienia właściwości, którą określa się „na podstawie prawa wewnętrznego". Dlatego konwencja powołuje się na krajowe przepisy dotyczące ochrony danych, które zgodnie z uzasadnieniem miałyby zawierać „dokładne kryteria określające, kto jest właściwą osobą".

Pierwszy wniosek Komisji odzwierciedla ten przepis, natomiast zmieniony wniosek Komisji odnosi się do organu „który decyduje", eliminując tym samym potrzebę określania właściwości na mocy prawa: określanie na mocy prawa jest nadal możliwe, chociaż nie jest konieczne. Potwierdzają to wspólne stanowisko Rady i przyjęty tekst, z które w obu przypadkach odnoszą się do organu „który określa".

W tym kontekście zmiany historyczne uwydatniają dwa ważne elementy: po pierwsze, można być administratorem danych niezależnie od szczególnych właściwości lub uprawnień do kontrolowania danych powierzonych na mocy prawa; po drugie, w procesie przyjmowania dyrektywy 95/46 określanie administratora danych stało się pojęciem wspólnotowym, które ma własne niezależne znaczenie w prawie wspólnotowym, niepodlegające zmianom z uwagi na ewentualnie rozbieżne przepisy prawa krajowego. Ten ostatni element ma zasadnicze znaczenie dla zapewnienia skutecznego stosowania dyrektywy i wysokiego poziomu ochrony w państwach członkowskich, który wymaga jednolitej, a zatem autonomicznej interpretacji kluczowego pojęcia, jakim jest „administrator danych". Pojęcie to nabrało w dyrektywie znaczenia, którego nie miało w konwencji nr 108.

Z tej perspektywy dyrektywa dopełnia tej ewolucji, stanowiąc, że chociaż zdolność „określania" może zostać nadana z mocy prawa, zwykle będzie wynikać z analizy elementów faktycznych lub okoliczności danego przypadku: należy przyjrzeć się konkretnym operacjom przetwarzania i zrozumieć, kto je określa, odpowiadając na pierwszym etapie na pytania „dlaczego dane przetwarzanie ma miejsce? Kto je rozpoczął?".

Bycie administratorem danych wynika przede wszystkim z okoliczności faktycznej, w której podmiot podjął decyzję o przetwarzaniu danych osobowych dla własnych celów. Wyłącznie formalne kryterium nie byłoby rzeczywiście wystarczające co najmniej z dwóch powodów: w niektórych przypadkach brakować będzie formalnego wyznaczenia administratora danych, określonego na przykład na mocy prawa w umowie lub w powiadomieniu skierowanym do organu ochrony danych; w innych przypadkach może się zdarzyć, że formalne wyznaczenie nie będzie odzwierciedlało rzeczywistości w przypadku formalnego powierzenia roli administratora danych organowi, który nie jest w stanie „określać".

Znaczenie wpływu faktycznego pokazuje także sprawa SWIFT[10], w której SWIFT uznano formalnie za przetwarzającego dane, ale w rzeczywistości działał on – przynajmniej w pewnym zakresie – jako administrator danych. W tym przypadku wyjaśniono, że chociaż wyznaczenie strony na administratora danych lub przetwarzający w umowie może ujawnić istotne informacje dotyczące statusu prawnego tej strony, wyznaczenie na mocy umowy nie jest jednak decydujące przy określaniu rzeczywistego statusu, które musi być oparty na konkretnych okolicznościach.

Podejście oparte na faktach poparte także okoliczność, że dyrektywa stanowi, iż administrator danych jest osobą, która „określa", a nie „zgodnie z prawem określa" cel i sposoby. Decydujące znaczenie ma skuteczne zidentyfikowanie sprawowania kontroli, nawet jeżeli wyznaczenie wydaje się niezgodne z prawem lub przetwarzanie danych odbywa się w sposób niezgodny z prawem. Nieistotne jest to, czy decyzja o przetwarzaniu danych była „zgodna z prawem", co oznacza, że podmiot podejmujący taką decyzję posiadał zdolność prawną do jej podjęcia lub administratora danych wyznaczono formalnie zgodnie ze specjalną procedurą. Kwestia zgodności przetwarzania danych osobowych z prawem będzie istotna na innym etapie i oceniana w świetle innych artykułów (w szczególności art. 6-8) dyrektywy. Innymi słowy ważne jest, aby nawet w

[10] Sprawa dotyczy przekazania władzom Stanów Zjednoczonych w celu zwalczania finansowania terroryzmu danych bankowych zgromadzonych przez SWIFT w ramach przeprowadzania transakcji finansowych w imieniu banków i instytucji finansowych.

przypadkach przetwarzania danych niezgodnego z prawem zapewnić możliwość łatwego odnalezienia administratora danych i uznania go za odpowiedzialnego za przetwarzanie.

Ostatnią cechą charakterystyczną pojęcia administratora danych jest jego autonomia, co oznacza, że chociaż zewnętrzne źródła prawne mogą być pomocne w ustaleniu, kto jest administratorem danych, interpretacji należy dokonywać przede wszystkim zgodnie z przepisami dotyczącymi ochrony danych[11]. Pojęcia administratora danych nie powinny naruszać inne, często kolidujące lub pokrywające się, pojęcia z innych dziedzin prawa, takie jak twórca lub posiadacz praw w prawach własności intelektualnej. Bycie posiadaczem praw własności intelektualnej nie wyklucza możliwości bycia uznanym także za „administratora danych", a zatem podlegania obowiązkom wynikającym z przepisów dotyczących ochrony danych.

Potrzeba typologii

Pojęcie administratora danych jest pojęciem funkcjonalnym, mającym na celu przypisanie obowiązków tam, gdzie występuje faktyczny wpływ, a zatem raczej w oparciu o analizę okoliczności faktycznych niż o analizę formalną. Określenie kontroli może zatem wymagać niekiedy szczegółowej i długiej analizy. Potrzeba zapewnienia skuteczności wymaga jednak pragmatycznego podejścia gwarantującego przewidywalność w odniesieniu do kontroli. W tym kontekście potrzebne są ogólne zasady i praktyczne przesłanki w celu zapewnienia wytycznych i ułatwienia stosowania przepisów dotyczących ochrony danych.

Wymaga to takiej interpretacji dyrektywy, która zapewni w większości sytuacji łatwą i jasną identyfikację „organu określającego" przez odniesienie do okoliczności prawnych lub faktycznych, z których normalnie może wynikać faktyczny wpływ, o ile inne elementy nie wskazują inaczej.

Okoliczności te można poddać analizie i sklasyfikować według następujących trzech kategorii sytuacji, które umożliwiają systematyczne podejście do tych kwestii:

1) *Kontrola wynikająca z wyraźnej kompetencji prawnych*. Odnosi się do niej między innymi druga część definicji, tj. przypadek, gdy administrator danych lub szczegółowe kryteria potrzebne do jego wyznaczenia są określane przez przepisy prawa krajowego lub wspólnotowego. Bezpośrednie wyznaczanie administratora danych na mocy prawa zwykle nie stwarza większych problemów. W niektórych krajach przepisy prawa krajowego przewidują, że władze publiczne odpowiadają za przetwarzanie danych osobowych w ramach swoich obowiązków.

Częściej ma jednak miejsce sytuacja, w której przepisy prawa, zamiast bezpośrednio wyznaczyć administratora danych lub określić kryteria jego wyznaczania, ustalają zadanie lub nakładają na kogoś obowiązek gromadzenia i przetwarzania niektórych danych. Tak może być na przykład w przypadku podmiotu, któremu powierzono pewne zadania publiczne (np. zabezpieczenie społeczne), których nie można wypełnić bez zgromadzenia przynajmniej niektórych danych osobowych, i który w celu wypełnienia tych zadań tworzy rejestr. W takim przypadku określenie, kto jest kontrolerem, wynika z prawa. Ogólniej mówiąc, prawo może nałożyć na podmioty publiczne lub prywatne

[11] Zob. poniżej, kolizja z pojęciami istniejącymi w innych dziedzinach prawa (na przykład pojęcie posiadacza praw do własności intelektualnej lub badań naukowych lub odpowiedzialność w świetle prawa cywilnego).

obowiązek zachowywania lub dostarczania niektórych danych. Podmioty te zazwyczaj byłyby uważane za administratorów danych w odniesieniu do przetwarzania danych osobowych w takim kontekście.

2) *Kontrola wynikająca z dorozumianej kompetencji*. Ma ona miejsce w przypadku, gdy prawo nie ustala wyraźnie zdolności do określania ani nie jest ona bezpośrednią konsekwencją wyraźnych przepisów prawnych, ale nadal wynika ze wspólnych przepisów prawnych lub utrwalonej praktyki dotyczącej różnych dziedzin (prawo cywilne, prawo handlowe, prawo pracy itd.). W takim przypadku w zidentyfikowaniu administratora danych pomogą istniejące tradycyjne role, które zwykle wiążą się z pewną odpowiedzialnością: będzie nim na przykład pracodawca w odniesieniu do danych dotyczących jego pracowników, wydawca w odniesieniu do danych dotyczących abonentów, stowarzyszenie w odniesieniu do danych dotyczących jego członków lub osób wspierających.

We wszystkich tych przypadkach zdolność określania działalności związanej z przetwarzaniem można uznać za powiązaną w sposób naturalny z funkcjonalną rolą organizacji (prywatnej), ostatecznie nakładającą odpowiedzialność także z punktu widzenia ochrony danych. Z prawnego punktu widzenia miałoby to zastosowanie niezależnie od faktu, czy zdolność określania zostanie nadana wspomnianym podmiotom prawnym, czy będzie realizowana przez odpowiednie organy działające w ich imieniu, czy przez osobę fizyczną pełniącą podobną rolę (zob. poniżej pierwszy element w pkt c). Taka sama sytuacja będzie jednak miała miejsce w przypadku organu publicznego wypełniającego pewne zadania administracyjne w kraju, w którym przepisy prawne nie określają jednoznacznie jego odpowiedzialności w zakresie przetwarzania danych.

Przykład nr 1: dostawcy usług telekomunikacyjnych

Ciekawy przykład wytycznych prawnych dla sektora prywatnego dotyczy roli dostawców usług telekomunikacyjnych: motyw 47 dyrektywy 95/46/WE wyjaśnia, że „w przypadku przekazywania komunikatu zawierającego dane osobowe przy pomocy urządzeń telekomunikacyjnych lub poczty elektronicznej, których wyłącznym przeznaczeniem jest przekazywanie takich komunikatów, za administratora danych osobowych zawartych w takim komunikacie uważać się będzie osobę, od której komunikat wychodzi, nie zaś osobę wykonującą usługę w zakresie transmisji danych; podmioty wykonujące takie usługi są z reguły uważane za administratorów danych w odniesieniu do przetwarzania dodatkowych danych osobowych potrzebnych do wykonywania usług". Dostawcę usług telekomunikacyjnych należy zatem uważać co do zasady za administratora danych jedynie w przypadku danych o ruchu i danych bilingowych, a nie wszystkich przekazywanych danych[12]. Powyższe wytyczne prawne prawodawcy wspólnotowego są w pełni zgodne z przyjętym w niniejszej opinii podejściem funkcjonalnym.

[12] Organ ochrony danych przeprowadził kontrolę w sprawie zgłoszonej przez osobę, której dane dotyczą, skarżącą się na reklamy przesyłane pocztą elektroniczną. W skardze osoba, której dane dotyczą, wystąpiła z wnioskiem, aby dostawca sieci łączności potwierdził lub zaprzeczył, że był nadawcą reklam przesyłanych pocztą elektroniczną. Organ ochrony danych stwierdził, że nie można uznać za administratora danych przedsiębiorstwa zapewniającego klientowi wyłącznie dostęp do sieci łączności, tj. takiego, które nie inicjuje przekazywania danych ani nie wybiera adresów i nie modyfikuje informacji zawartych w przekazywanych danych.

3) *Kontrola wynikająca z faktycznego wpływu*. Ma ona miejsce w przypadku, gdy funkcję administratora danych przydziela się na podstawie oceny okoliczności faktycznych. W wielu przypadkach będzie się to wiązało z oceną stosunków umownych między różnymi zaangażowanymi stronami. Ocena pozwala na wyciągnięcie zewnętrznych wniosków, przydzielenie roli i obowiązków administratora danych co najmniej jednej ze stron. Może być to szczególnie przydatne w skomplikowanych środowiskach, korzystających często z nowych technologii informacyjnych, w których odpowiednie podmioty są często skłonne postrzegać się jako „pośrednicy", a nie jako odpowiedzialni administratorzy danych.

Może się zdarzyć, że w umowie nie wspomniano, kto jest administratorem danych, ale zawarto elementy wystarczające do przydzielenia funkcji administratora danych stronie, która najwyraźniej pełni dominującą rolę w tym zakresie. Może zdarzyć się również, że umowa bardziej precyzyjnie określa administratora danych. Jeżeli nie ulega wątpliwości, że odzwierciedla to dokładnie rzeczywistość, nic nie stoi na przeszkodzie wypełnienia warunków umowy. Jednak nie we wszystkich okolicznościach warunki umowy mają decydujące znaczenie, ponieważ umożliwiłoby to stronom przydzielanie obowiązków w dogodny dla siebie sposób.

Sam fakt określania przez kogoś sposobu przetwarzania danych osobowych może kwalifikować go jako administratora danych, chociaż taka kwalifikacja powstaje poza zakresem stosunku umownego lub jest wyraźnie wykluczona w umowie. Wyraźnych przykładem takiej sytuacji była sprawa SWIFT, w której omawiane przedsiębiorstwo postanowiło udostępnić niektóre dane osobowe – początkowo przetwarzane dla celów handlowych w imieniu instytucji finansowych – również w celu zwalczania finansowania terroryzmu, zgodnie z wezwaniami Departamentu Skarbu Stanów Zjednoczonych.

W przypadku wątpliwości w celu znalezienia administratora danych przydatne mogą być elementy inne niż warunki umowy, jak na przykład poziom faktycznej kontroli sprawowanej przez stronę, obraz przekazywany osobom, których dane dotyczą, i uzasadnione oczekiwania osób, których dane dotyczą, oparte na tej widoczności (zob. także trzeci element w pkt b) poniżej). Kategoria ta jest szczególnie ważna, ponieważ umożliwia odniesienie się do obowiązków i powierzenie ich także w przypadkach postępowania niezgodnego z prawem, w których faktyczna działalność związana z przetwarzaniem może być prowadzona wbrew interesom i woli niektórych stron.

Wniosek wstępny

Wśród tych kategorii pierwsze dwie pozwalają zasadniczo na bezpieczniejsze wskazywanie organu określającego i mogą obejmować w praktyce ponad 80 % odnośnych sytuacji. Jednak formalne wyznaczenie prawne powinno być zgodne z przepisami dotyczącymi ochrony danych poprzez zapewnienie skutecznej kontroli operacji przetwarzania przez wyznaczony organ lub, innymi słowy, poprzez zapewnienie, że wyznaczenie na mocy prawa odzwierciedla stan rzeczy.

Kategoria 3 wymaga bardziej złożonej analizy i może prowadzić do rozbieżnych interpretacji. Warunki umowy mogą często pomagać w wyjaśnieniu kwestii, ale nie we wszystkich okolicznościach są decydujące. Istnieje coraz więcej podmiotów, które nie uważają się za określające działalność związaną z przetwarzaniem, a tym samym za odpowiedzialne za nią. Wniosek oparty na wpływie faktycznym jest w tych przypadkach

jedynym wykonalnym wariantem. Kwestia legalności takiego przetwarzania będzie nadal oceniana w świetle innych artykułów (6–8).

Jeżeli żadna z wyżej wymienionych kategorii nie znajdzie zastosowania, wyznaczanie administratora danych należy uważać za nieważne. Organu, który nie ma prawnego ani faktycznego wpływu na określanie sposobu przetwarzania danych osobowych, nie można uważać za administratora danych.

Z formalnego punktu widzenia podejście to potwierdza fakt, że definicję administratora danych należy uważać za obligatoryjny przepis prawny, od którego strony nie mogą zwyczajnie odstąpić lub uchylić się. Z perspektywy strategicznej takie wyznaczenie może stać w sprzeczności ze skutecznym stosowaniem przepisów dotyczących ochrony danych i unieważnić odpowiedzialność związaną z przetwarzaniem danych.

III.1.b) Trzeci element: „cele i sposoby przetwarzania”

Trzeci element stanowi ważną część testu: co strona powinna określić, aby uznano ją za administratora danych.

Historia tego przepisu pokazuje wiele zmian. Konwencja nr 108 odnosiła się do celu zbiorów zautomatyzowanych, kategorii danych osobowych i stosowanych na nich operacji. Komisja przejęła te istotne elementy z niewielkimi zmianami językowymi i uzupełniła je o kompetencje do podejmowania decyzji w kwestii, które osoby trzecie mogą mieć dostęp do danych. Zmieniony wniosek Komisji stanowił krok naprzód w kierunku przejścia od „celu zbioru danych” do „celów i sposobów przetwarzania”, a zatem przejście od statycznej definicji związanej ze zbiorem danych do definicji dynamicznej związanej z czynnością przetwarzania danych. Zmieniony wniosek nadal odnosił się do czterech elementów (cele, dane osobowe, operacje i osoby trzecie mające do nich dostęp), które we wspólnym stanowisku Rady ograniczono jedynie do dwóch („cele i sposoby”).

Słowniki definiują „cel” jako „oczekiwany rezultat, który jest zamierzony lub który kieruje zaplanowanymi działaniami”, a „sposób” jako „określenie sposobu osiągnięcia rezultatu lub celu”.

Z drugiej strony dyrektywa stanowi, że dane są gromadzone do określonych, jednoznacznych i legalnych celów oraz nie są poddawane dalszemu przetwarzaniu w sposób niezgodny z tym celem. Dlatego szczególne znaczenie ma określenie „celów” przetwarzania i „sposobów” ich osiągnięcia.

Można również stwierdzić, że określanie celów i sposobów sprowadza się do określenia odpowiednio „dlaczego” i „jak” prowadzi się pewne czynności przetwarzania danych. W tym kontekście, a także uwzględniając współistnienie obydwu elementów, istnieje potrzeba zapewnienia wytycznych wyjaśniających, jak duży wpływ na „dlaczego” i „jak” może mieć uznanie podmiotu za administratora danych.

Przy dokonywaniu oceny określania celów i sposobów zmierzających do przydzielenia roli administratora danych, kluczowym zagadnieniem jest zatem to, jak szczegółowo należy określać cele i sposoby uznania za administratora danych. W związku z tym również, jaki jest margines działania, który dyrektywa przyznaje przetwarzającemu dane. Definicje te stają się szczególnie istotne, gdy w przetwarzanie danych osobowych zaangażowane są różne podmioty i konieczne jest określenie, który z nich jest

administratorem danych (sam lub wraz z innymi), a które należy uważać za przetwarzających dane, o ile występują.

Nacisk kładziony na cele lub sposoby może być różny w zależności od konkretnego kontekstu, w jakim odbywa się przetwarzanie.

Potrzebne jest podejście pragmatyczne, które większy nacisk kładzie na swobodę w określaniu celów i na uznaniowość w podejmowaniu decyzji. W tych przypadkach chodzi o to, dlaczego prowadzi się przetwarzanie i jaka jest rola ewentualnych podmiotów powiązanych, takich jak przedsiębiorstwa outsourcingowe: czy przedsiębiorstwo outsourcingowe przetwarzałoby dane, gdyby nie poprosił o to administrator danych i na jakich warunkach? Przetwarzający mógłby działać dalej zgodnie z ogólnymi wytycznymi, które dotyczą przede wszystkim celów i nie wnikają szczegółowo w kwestię sposobów.

Przykład nr 2: marketing mailowy

Przedsiębiorstwo ABC zawiera umowy z różnymi organizacjami w celu prowadzenia kampanii marketingu mailowego i prowadzenia listy płac. Wydaje jasne instrukcje (jakie materiały marketingowe wysyłać i do kogo, komu płacić, jakie kwoty, do kiedy itd.). Chociaż organizacjom przysługuje pewna swoboda (w tym w kwestii, jakie oprogramowanie stosować), ich zadania są dość jasno i ściśle określone, i mimo że firma mailingowa może udzielać porad (np. odradzać wysyłanie przesyłek reklamowych w sierpniu), organizacje są zobowiązane postępować zgodnie z instrukcjami ABC. Ponadto tylko jeden podmiot, przedsiębiorstwo ABC, jest uprawniony do korzystania z przetwarzanych danych – wszystkie inne podmioty muszą opierać się na podstawie prawnej przedsiębiorstwa ABC w przypadku zakwestionowania ich zdolności prawnej do przetwarzania danych. W tym przypadku jasne jest, że przedsiębiorstwo ABC jest administratorem danych, a każdą z odrębnych organizacji można uznać za przetwarzający w odniesieniu do konkretnego przetwarzania danych prowadzonego w jego imieniu.

Jeżeli chodzi o określanie sposobów, termin „sposób” w sposób oczywisty obejmuje zupełnie różne elementy, co również ilustruje historia tej definicji. W pierwotnym wniosku rola administratora danych wynikałaby z określenia czterech elementów (celów, danych osobowych, operacji i osób trzecich mających do nich dostęp). Ostatecznej wersji przepisu, odnoszącej się tylko do „celów i sposobów”, nie można interpretować jako sprzecznej ze starszą wersją, ponieważ nie ma wątpliwości co do faktu, że np. do administratora danych należy określenie, które dane przetwarza się w zamierzonym celu (zamierzonych celach). Ostateczną wersję definicji należy zatem rozumieć wyłącznie jako skróconą wersję zawierającą jednak sens wersji starszej. Innymi słowy „sposoby” nie odnoszą się tylko do technicznych sposobów przetwarzania danych osobowych, ale także do tego „jak” odbywa się przetwarzanie, co obejmuje zagadnienia „które dane się przetwarza”, „jakie osoby trzecie mają dostęp do tych danych”, „kiedy usuwa się dane" itd.

Określanie „sposobów” obejmuje zatem zarówno kwestie techniczne i organizacyjne, gdy podejmowanie decyzji można przekazać przetwarzającym (np. „z jakiego sprzętu komputerowego i oprogramowania korzystać?”), jak i zasadnicze elementy, które w tradycyjny i nieodłączny sposób określa administrator danych, takie jak „które dane się przetwarza?”, „jak długo się je przetwarza?”, „kto ma do nich dostęp?” itd.

W tym kontekście, chociaż określanie celu przetwarzania w każdym przypadku spowodowałoby uznanie za administratora danych, określanie sposobów wiązałoby się z kontrolą jedynie w przypadku, gdy określanie dotyczy zasadniczych elementów przedmiotowych sposobów.

Z tej perspektywy możliwe jest, że sposoby techniczne i organizacyjne są określanie wyłącznie przez administratora danych.

W tych przypadkach – gdy istnieje dobra definicja celów, ale jest niewiele lub nie ma w ogóle wytycznych dotyczących sposobów technicznych i organizacyjnych – sposoby powinny reprezentować uzasadnioną drogę osiągania celu (celów), a administratora należy dokładnie poinformować o wykorzystanych sposobach. Jeżeli wykonawca ma wpływ na cel i prowadzi przetwarzanie (również) dla własnych korzyści, na przykład wykorzystując dane osobowe otrzymane w celu tworzenia usług dodanych, jest on administratorem danych (lub ewentualnie wspólnym administratorem danych) dla innej czynności przetwarzania danych, a zatem podlega wszystkim zobowiązaniom wynikającym z właściwych przepisów o ochronie danych.

Przykład nr 3: przedsiębiorstwo nazywane przetwarzającym, ale występujące w charakterze administratora danych

Przedsiębiorstwo MarketinZ świadczy usługi z zakresu reklamy promocyjnej i marketingu bezpośredniego dla różnych firm. Przedsiębiorstwo GoodProductZ zawiera umowę z MarketinZ, zgodnie z którą przedsiębiorstwo MarketinZ świadczy usługi reklamy komercyjnej dla klientów GoodProductZ i jest nazywane przetwarzającym dane. MarketinZ postanawia jednak wykorzystać bazę danych klientów GoodProductZ również w celu promowania produktów innych klientów. Decyzja, aby dołączyć dodatkowy cel do celu, w którym przekazano dane osobowe, zmienia MarketinZ w administratora danych dla celów danej operacji przetwarzania. Kwestia zgodności przetwarzania z prawem zostanie oceniona w świetle innych artykułów (6–8).

W niektórych systemach prawnych decyzje dotyczące środków bezpieczeństwa mają szczególnie duże znaczenie, ponieważ środki bezpieczeństwa uznaje się bezpośrednio za podstawową właściwość określaną przez administratora danych. Podnosi to kwestię, które decyzje dotyczące bezpieczeństwa mogą spowodować uznanie przedsiębiorstwa, któremu zlecono przetwarzanie, za administratora danych.

Wniosek wstępny

Określenie „celu” przetwarzania jest zastrzeżone dla „administratora danych”. Ktokolwiek podejmuje tę decyzję jest (faktycznie) administratorem danych. Administrator danych może przekazać określanie „sposobów” przetwarzania w odniesieniu do kwestii technicznych lub organizacyjnych. Zasadnicze kwestie dotyczące sedna zgodności przetwarzania danych z prawem należą do administratora danych. Osoba lub podmiot, które podejmują decyzję dotyczącą np. tego, jak długo przechowuje się dane lub kto ma dostęp do przetworzonych danych, działają jako „administrator danych” w odniesieniu do tej części wykorzystywania danych, a zatem muszą spełniać wszystkie obowiązki administratora danych.

III.1.c) Pierwszy element: „osoba fizyczna, osoba prawna lub inny organ”

Pierwszy element definicji odnosi się do aspektu personalnego: kto może być administratorem danych, a więc kogo ostatecznie można uznać za odpowiedzialnego za pełnienie obowiązków wynikających z dyrektywy. Definicja odzwierciedla dokładnie brzmienie art. 2 konwencji 108 i nie była przedmiotem odrębnej dyskusji w procesie uzgadniania dyrektywy. Odnosi się ona do zbioru obszernej grupy podmiotów, które mogą pełnić rolę administratora danych, począwszy od osób fizycznych po osoby prawne, w tym „każdy inny organ”.

Ważne jest, aby wykładnia tego elementu zapewniała skuteczne stosowanie dyrektywy, sprzyjając w jak największym stopniu wyraźnej i jednoznacznej identyfikacji administratora danych we wszystkich okolicznościach, bez względu na to, czy nastąpiło formalne wyznaczenie i zostało to podane do wiadomości publicznej.

Przede wszystkim ważne jest, by w miarę możliwości nie odstępować od praktyki utrwalonej w sektorze publicznym i prywatnym zgodnie z innymi dziedzinami prawa, jak prawo cywilne, administracyjne i karne. W większości przypadków przepisy te wskażą, jakim osobom lub organom należy przydzielić obowiązki, i zasadniczo pomogą ustalić, kto jest administratorem danych.

W strategicznym kontekście powierzania obowiązków i w celu zapewnienia osobom, których dane dotyczą, bardziej stabilnego i niezawodnego podmiotu referencyjnego przy wykonywaniu swoich praw zgodnie z dyrektywą, za administratora danych należy uznać raczej przedsiębiorstwo jako takie lub organ jako taki, niż konkretną osobę w przedsiębiorstwie lub organie. To właśnie przedsiębiorstwo lub organ ostatecznie uznaje się za odpowiedzialne za przetwarzanie danych i wypełnianie obowiązków wynikających z przepisów o ochronie danych, chyba że istnieją wyraźne elementy wskazujące, że odpowiedzialna jest osoba fizyczna. Należy na ogół zakładać, że przedsiębiorstwa lub organy publiczne są jako takie odpowiedzialne za czynności związane z przetwarzaniem danych odbywające się w ramach ich działań i ryzyka.

Niekiedy przedsiębiorstwa i organy publiczne wyznaczają konkretną osobę odpowiedzialną za prowadzenie czynności przetwarzania danych. Jednak również w przypadku, gdy konkretna osoba fizyczna jest wyznaczana w celu zapewnienia zgodności z zasadami ochrony danych lub w celu przetwarzania danych osobowych, nie będzie ona administratorem danych, natomiast będzie występować w imieniu osoby prawnej (przedsiębiorstwa lub organu publicznego), która nadal będzie ponosiła odpowiedzialność w razie naruszenia zasad jako administrator danych[13].

Szczególnie w przypadku dużych i złożonych struktur kluczową kwestią „zarządzania ochroną danych” jest zapewnienie zarówno wyraźnej odpowiedzialności osoby fizycznej reprezentującej przedsiębiorstwo, jak i konkretnego funkcyjnego zakresu obowiązków w ramach struktury, na przykład poprzez powierzenie innym osobom roli przedstawicieli lub osób wyznaczonych do kontaktów z osobami, których dane dotyczą.

[13] Podobne rozumowanie ma zastosowanie w odniesieniu do rozporządzenia (WE) 45/2001, którego art. 2 lit. d) odnosi się do „instytucji lub organu Wspólnoty, dyrekcji generalnej, oddziału lub jakiejkolwiek innej jednostki organizacyjnej”. W praktyce nadzoru wyraźnie ustalono, że urzędnicy instytucji i organów UE, którzy zostali wyznaczeni na „administratorów danych”, działają w imieniu organu, dla którego pracują.

W przypadkach, w których osoba fizyczna działająca w obrębie osoby prawnej wykorzystuje dane dla własnych celów nieobjętych zakresem i ewentualną kontrolą działalności osoby prawnej, niezbędna jest specjalna analiza. W takiej sytuacji dana osoba fizyczna byłaby administratorem przetwarzania danych, co do którego podjęła decyzję, i ponosiłaby odpowiedzialność za takie wykorzystanie danych osobowych. Pierwotny administrator danych mógłby jednak ponosić pewną odpowiedzialność w przypadku, jeżeli nowe przetwarzanie danych miałoby miejsce na skutek braku odpowiednich środków bezpieczeństwa.

Jak już wspomniano powyżej, rola administratora danych jest kluczowa i szczególnie istotna, gdy chodzi o ustalenie odpowiedzialności i stosowanie sankcji. Nawet jeżeli odpowiedzialność i sankcje będą się różnić w zależności od państwa członkowskiego, ponieważ są stosowane zgodnie z przepisami krajowymi, potrzeba wyraźnej identyfikacji osoby fizycznej lub prawnej odpowiedzialnej za naruszenie przepisów o ochronie danych osobowych jest bez wątpienia zasadniczym warunkiem koniecznym dla skutecznego stosowania dyrektywy.

Identyfikacja „administratora danych" w kontekście ochrony danych będzie w praktyce wiązać się z przepisami prawa cywilnego, administracyjnego lub karnego odnoszącymi się do powierzania obowiązków lub stosowania sankcji, którym osoba fizyczna lub prawna może podlegać[14].

Odpowiedzialność cywilna nie powinna nastręczać szczególnych problemów w tym kontekście, ponieważ zasadniczo ma zastosowanie zarówno do osób fizycznych, jak i prawnych. Odpowiedzialność karna lub administracyjna może jednak niekiedy mieć zastosowanie, zgodnie z przepisami krajowymi, jedynie do osób fizycznych. Jeśli zgodnie z odpowiednimi przepisami krajowymi istnieją sankcje karne lub administracyjne za naruszenie zasad ochrony danych, przepisy te będą zazwyczaj stanowić, kto ponosi odpowiedzialność: w przypadkach, w których odpowiedzialność karna lub administracyjna osób prawnych nie jest uznawana, odpowiedzialność tak a mogą ponosić członkowie kierownictwa osób prawnych zgodnie ze szczególnymi przepisami prawa krajowego[15].

W prawie europejskim występują przydatne przykłady kryteriów przypisujących odpowiedzialność karną[16], w szczególności w przypadku, gdy przestępstwo zostaje popełnione z korzyścią dla osoby prawnej: w takim przypadku odpowiedzialność można przypisać każdej osobie „zajmującej pozycję kierowniczą w strukturze osoby prawnej, działającej indywidualnie lub jako członek organu osoby prawnej, w oparciu o:
a) prawo do reprezentowania osoby prawnej;

---

14 Zob. opracowane przez Komisję „Badanie porównawcze sytuacji w 27 państwach członkowskich pod względem przepisów mających zastosowanie do pozaumownych zobowiązań powstających w wyniku naruszenia prywatności i praw odnoszących się do osobowości", luty 2009 r., dostępne pod adresem: http://ec.europa.eu/justice_home/doc_centre/civil/studies/doc/study_privacy_en.pdf

15 Nie wyklucza to możliwości ustanowienia w przepisach krajowych odpowiedzialności karnej lub administracyjnej nie tylko wobec administratora danych, ale również wobec każdej osoby naruszającej przepisy o ochronie danych.

16 Zob. np. Dyrektywa 2008/99/WE z dnia 19 listopada 2008 r. w sprawie ochrony środowiska poprzez prawo karne, decyzja ramowa Rady z dnia 13 czerwca 2002 r. w sprawie zwalczania terroryzmu. Instrumenty prawne opierają się na art. 29, art. 31 lit. e) i art. 34 ust. 2 lit. b) TUE albo odpowiadają podstawom prawnym instrumentów stosowanych w pierwszym filarze, wynikających z orzecznictwa Trybunału Sprawiedliwości w sprawach C-176/03 *Komisja przeciwko Radzie*, Rec. 2005 r. s. I-7879 oraz C-440/05 *Komisja przeciwko Radzie*, Rec. z 2007 s. I-9097. Zobacz również komunikat COM (2005) 583 wersja ostateczna.

b) uprawnienia do podejmowania decyzji w imieniu osoby prawnej; lub
c) uprawnienia do sprawowania kontroli w strukturach osoby prawnej".

Wstępny wniosek

Podsumowując powyższe rozważania można stwierdzić, że za naruszenie ochrony danych odpowiedzialny jest zawsze administrator danych, tj. osoba prawna (przedsiębiorstwo lub organ publiczny) lub osoba fizyczna, formalnie zidentyfikowana zgodnie z kryteriami dyrektywy. Jeśli osoba prawna pracująca w przedsiębiorstwie lub organie publicznym wykorzystuje dane dla własnych celów nieobjętych działalnością przedsiębiorstwa, osobę tę uznaje się za faktycznego administratora danych i jako taki zostanie ona pociągnięta do odpowiedzialności.

Przykład nr 4: potajemne monitorowanie pracowników

Członek zarządu przedsiębiorstwa podejmuje decyzję o potajemnym monitorowaniu pracowników przedsiębiorstwa, choć decyzja ta nie jest formalnie zatwierdzona przez zarząd. Przedsiębiorstwo należy uznać za administratora danych i liczyć się z ewentualnymi roszczeniami i odpowiedzialnością wobec pracowników, których dane osobowe zostały niewłaściwe wykorzystane.

Odpowiedzialność przedsiębiorstwa wynika w szczególności z faktu, że jako administrator danych ma obowiązek zapewnić zgodność z zasadami bezpieczeństwa i poufności. Nadużycie ze strony członka kierownictwa przedsiębiorstwa lub pracownika można uznać za efekt nieodpowiednich środków bezpieczeństwa. Nie ma znaczenia, czy na późniejszym etapie również członek zarządu lub inne osoby fizyczne w przedsiębiorstwie mogą być uznani za odpowiedzialnych, zarówno z punktu widzenia prawa cywilnego − również w stosunku do przedsiębiorstwa − jak i z punktu widzenia prawa karnego. Mogłoby to mieć miejsce np. gdyby członek zarządu wykorzystywał zgromadzone dane do wymuszania na pracownikach osobistych korzyści: musiałby być uznany za „administratora danych" i obciążony odpowiedzialnością za to konkretne wykorzystanie danych.

III.1.d) Drugi element: „samodzielnie lub wspólnie z innymi podmiotami"

W niniejszym akapicie, na podstawie wcześniejszej analizy typowych cech administratora danych, omówione zostaną przypadki, w których przy przetwarzaniu danych osobowych oddziałuje na siebie wiele podmiotów. Rośnie bowiem liczba przypadków, w których różne podmioty funkcjonują jako administratorzy danych, i ten fakt uwzględniono w definicji zamieszczonej w dyrektywie.

Możliwości, że administrator danych działa „samodzielnie lub wspólnie z innymi podmiotami" nie uwzględniono w konwencji 108 i została ona w rzeczywistości wprowadzona dopiero przez Parlament Europejski przed przyjęciem dyrektywy. W swojej opinii w sprawie poprawki Parlamentu Europejskiego Komisja odniosła się do możliwości, zgodnie z którą „»w pojedynczej operacji przetwarzania danych kilka stron może wspólnie określić cel i sposoby przewidywanego przetwarzania danych«, a w związku z tym w takim przypadku »należy uznać, że na każdego współadministratora danych nałożone są ograniczenia wynikające z określonych w dyrektywie obowiązków w zakresie ochrony osób fizycznych, których dotyczą przetwarzane dane«".

Opinia Komisji nie odzwierciedliła w pełni złożoności obecnych realiów w zakresie przetwarzania danych, ponieważ koncentrowała się jedynie na przypadku, w którym wszyscy administratorzy w równym stopniu decydują o pojedynczej operacji przetwarzania danych i są w równym stopniu za nią odpowiedzialni. Natomiast rzeczywistość pokazuje, że jest to tylko jeden z różnych rodzajów „pluralistycznej kontroli", jaka może mieć miejsce. W tym względzie „wspólnie" należy interpretować jako „razem z" lub „nie samodzielnie" w różnych formach i kombinacjach.

Po pierwsze należy zwrócić uwagę na fakt, iż prawdopodobieństwo, że w przetwarzanie danych osobowych będzie zaangażowanych wiele podmiotów jest w sposób naturalny powiązane z różnymi rodzajami działalności, które zgodnie z dyrektywą mogą być równoznaczne z „przetwarzaniem", będącym w ostatecznym rozrachunku przedmiotem „wspólnej kontroli". Definicja przetwarzania danych, o której mowa w art. 2 lit. b) dyrektywy, nie wyklucza możliwości, że różne podmioty są zaangażowane w różne operacje lub grupy operacji odnośnie do danych osobowych. Operacje te mogą mieć miejsce jednocześnie lub na różnych etapach.

W tak złożonym środowisku jeszcze bardziej istotne jest, by można było łatwo przypisać role i zakres obowiązków, aby złożoność wspólnej kontroli nie prowadziła do niewykonalnego podziału zakresu obowiązków, co obniżyłoby skuteczność przepisów o ochronie danych. Niestety, ze względu na różnorodność ewentualnych układów, nie ma możliwości sporządzenia wyczerpującej „zamkniętej" listy poszczególnych rodzajów „wspólnej kontroli" lub ich kategoryzacji. Przydatne jest jednak zapewnienie również w tym kontekście wytycznych w oparciu o pewne kategorie i przykłady wspólnej kontroli, a także pewne faktyczne elementy, z których wspólna kontrola może wynikać lub na podstawie których można założyć, że istnieje.

Ogólnie ocena wspólnej kontroli powinna odzwierciedlać ocenę „pojedynczej" kontroli, o której mowa powyżej w pkt III.1.a) − III.1.c). Również przy ocenie wspólnej kontroli należy przyjąć konkretne i funkcjonalne podejście, jak przedstawiono powyżej, koncentrując się na tym, czy cele i sposoby są określane przez więcej niż jedną stronę.

Przykład nr 5: instalacja kamer przemysłowych

Właściciel budynku zawiera umowę z firmą ochroniarską, w wyniku której firma instaluje kamery w różnych częściach budynku w imieniu administratora danych. Cele nadzoru wideo oraz sposób, w jaki gromadzi się i przechowuje obrazy, są określane wyłącznie przez właściciela budynku, którego z tego względu należy uznać za jedynego administratora danych w odniesieniu do tej operacji przetwarzania danych.

Również w tym kontekście zobowiązania umowne mogą być użyteczne przy ocenie wspólnej kontroli, ale należy zawsze uwzględnić faktyczne okoliczności dotyczące zależności pomiędzy stronami.

Przykład nr 6: łowcy głów

Przedsiębiorstwo Headhunterz Ltd pomaga Enterprize Inc w rekrutacji nowych pracowników. Umowa wyraźnie stanowi, że „Headhunterz Ltd działa w imieniu Enterprize i że przy przetwarzaniu danych osobowych działa jako przetwarzający. Enterprize jest „jedynym administratorem danych".

Sytuacja Headhunterz Ltd nie jest jednak jednoznaczna: z jednej strony pełni rolę administratora danych w stosunku do osób poszukujących pracy, z drugiej strony zakłada, że jest przetwarzającym, działającym w imieniu administratorów danych, takich jak Enterprize Inc i innych przedsiębiorstw poszukujących pracowników za jego pośrednictwem. Ponadto Headhunterz – wraz z jego słynną usługą dodaną „globalnego dopasowania" − szuka odpowiednich kandydatów zarówno wśród CV otrzymywanych bezpośrednio od Enterprize, jak i wśród tych, które już posiada w swojej obszernej bazie danych. Dzięki temu, Headhunterz, które zgodnie z umową otrzymuje wynagrodzenie tylko za faktycznie podpisane umowy, zwiększa dopasowanie ofert pracy do osób poszukujących pracy, zwiększając tym samym swoje dochody. Na podstawie powyższych informacji można stwierdzić, że mimo przypisanej mu roli w umowie Headhunterz Ltd należy uznać za administratora danych, który administruje wspólnie z Enterprize Inc przynajmniej tymi grupami operacji, które odnoszą się do rekrutacji Enterprize.

W tym kontekście wspólna kontrola będzie miała miejsce, gdy poszczególne strony określą w odniesieniu do konkretnych operacji przetwarzania danych cel lub te podstawowe elementy sposobów przetwarzania danych, które charakteryzują administratora danych (zob. powyżej pkt III.1.a) − III.1.c)).

W kontekście wspólnej kontroli udział stron we wspólnym określaniu celów i sposobów może jednak przyjąć różne formy i nie musi być równo rozłożony. W przypadku wielu podmiotów mogą one być bardzo ściśle ze sobą powiązane (mając, na przykład, wspólne wszystkie cele i sposoby przetwarzania) lub pozostawać w luźniejszych stosunkach (na przykład, mając tylko wspólne cele lub wspólne sposoby przetwarzania bądź ich część). W związku z tym należy uwzględnić dużą różnorodność rodzajów wspólnej kontroli i ocenić ich skutki prawne, dopuszczając pewną elastyczność, aby przygotować się na rosnącą złożoność obecnych realiów w zakresie przetwarzania danych.

W tym kontekście należy przyjrzeć się poszczególnym stopniom, w jakich różne strony mogą oddziaływać na siebie lub być ze sobą powiązane w trakcie przetwarzania danych osobowych.

Po pierwsze, sam fakt, że w procesie przetwarzania danych osobowych współpracują różne podmioty, na przykład w łańcuchu, nie oznacza, że są one wspólnymi administratorami we wszystkich przypadkach, ponieważ wymianę danych między dwiema stronami przy braku wspólnych celów lub sposobów przetwarzania w ramach wspólnej grupy operacji należy uważać wyłącznie za przekazywanie danych pomiędzy dwoma oddzielnymi administratorami danych.

Przykład nr 7: biuro podróży (1)

Biuro podróży przesyła dane osobowe swoich klientów do linii lotniczych i sieci hoteli, w celu rezerwacji pakietów turystycznych. Linia lotnicza i hotel potwierdzają dostępność żądanych miejsc. Biuro podróży wystawia dokumenty i potwierdzenia dla swoich klientów. W tym przypadku, biuro podróży, linia lotnicza i hotel będą trzema odrębnymi administratorami danych, z których każdy podlega obowiązkom ochrony danych w odniesieniu do przetwarzania danych osobowych we własnym zakresie.

Taka ocena może jednak ulec zmianie, jeżeli różne podmioty postanowią stworzyć wspólną infrastrukturę, każdy dla własnych indywidualnych celów. Gdy przy tworzeniu takiej infrastruktury podmioty te określą kluczowe elementy sposobów przetwarzania danych, które zostaną wykorzystane, kwalifikują się na wspólnych administratorów danych − przynajmniej w tym zakresie − nawet jeśli niekoniecznie podzielają takie same cele.

Przykład nr 8: biuro podróży (2)

Biuro podróży, sieć hoteli i linie lotnicze postanawiają założyć wspólną platformę internetową w celu udoskonalenia współpracy w zakresie zarządzania rezerwacjami turystycznymi. Uzgadniają ważne elementy sposobów przetwarzania danych, które będą stosowane, na przykład jakie dane będą przechowywane, w jaki sposób rezerwacja będzie przypisywana i zatwierdzana oraz kto może mieć dostęp do przechowywanych informacji. Postanawiają ponadto wymieniać się danymi swoich klientów w celu prowadzenia zintegrowanych działań marketingowych.

W tym przypadku biuro podróży, linia lotnicza i sieć hoteli będą sprawować wspólną kontrolę nad tym, w jaki sposób dane osobowe ich poszczególnych klientów będą przetwarzane, i dlatego będą wspólnymi administratorami danych w odniesieniu do operacji przetwarzania danych związanych ze wspólną internetową platformą rezerwacji. Każdy z tych podmiotów będzie jednak nadal sprawował wyłączną kontrolę nad innymi działaniami w zakresie przetwarzania danych, np. działaniami związanymi z zarządzaniem zasobami ludzkimi.

W niektórych przypadkach różne podmioty przetwarzają kolejno te same dane osobowe. W takich przypadkach możliwe jest, że w skali mikro poszczególne operacje przetwarzania danych w łańcuchu wydają się niepowiązane, ponieważ każda z nich może mieć inny cel. Należy jednak dwukrotnie sprawdzić, czy w skali makro nie należałoby operacji przetwarzania danych uznać za „grupę operacji" służących jednemu celowi lub wykorzystujących wspólnie określone sposoby przetwarzania danych.

Następujące dwa przykłady wyjaśnią tę koncepcję, przedstawiając dwa różne możliwe scenariusze.

Przykład nr 9: przekazywanie danych pracowniczych organom podatkowym

Przedsiębiorstwo XYZ gromadzi i przetwarza dane osobowe swoich pracowników w celu zarządzania płacami, podróżami służbowymi, ubezpieczeniami zdrowotnymi itp. Prawo nakłada jednak również na przedsiębiorstwo obowiązek przesyłania organom podatkowym wszystkich danych odnoszących się do płac w celu wzmocnienia kontroli fiskalnej.

W tym przypadku, chociaż zarówno przedsiębiorstwo XYZ, jak i organy podatkowe, przetwarzają te same dane odnoszące się do płac, brak wspólnego celu lub sposobów przetwarzania tych danych prowadzi do uznania tych dwóch podmiotów za dwóch odrębnych administratorów danych.

Przykład nr 10: transakcje finansowe

Przyjrzymy się teraz przypadkowi banku, który wykorzystuje operatora komunikatów finansowych do prowadzenia transakcji finansowych. Bank i operator uzgadniają sposoby przetwarzania danych finansowych. Przetwarzaniem danych osobowych odnoszących się do transakcji finansowych zajmuje się na pierwszym etapie instytucja finansowa, a dopiero na późniejszym − operator komunikatów finansowych. Nawet jeśli każdy z tych podmiotów w skali mikro zmierza do innego celu, to w skali makro poszczególne etapy, cele i sposoby przetwarzania danych są ściśle powiązane. W tym przypadku zarówno bank, jak i operatora komunikatów należy uznać za wspólnych administratorów danych.

Istnieją inne przypadki, w których różne zaangażowane podmioty wspólnie określają, niekiedy w różnym zakresie, cele lub sposoby przetwarzania danych.

Istnieją przypadki, w których każdy administrator danych jest odpowiedzialny tylko za część przetwarzania danych, ale wszystkie informacje są łączone i przetwarzane w ramach platformy.

Przykład nr 11: portale administracji elektronicznej

Portale administracji elektronicznej działają jako pośrednicy pomiędzy obywatelami a jednostkami administracji publicznej: portal przekazuje wnioski obywateli i przechowuje dokumenty jednostki administracji publicznej do chwili wycofania ich przez obywateli. Każda jednostka administracji publicznej pozostaje administratorem danych przetwarzanych do jej własnych celów. Niemniej jednak sam portal również można uznać za administratora danych. Przetwarza on bowiem (tj. gromadzi i przekazuje właściwej jednostce) wnioski obywateli oraz publiczne dokumenty (tj. przechowuje je i reguluje do nich dostęp, jak pobieranie ich przez obywateli) do innych celów (ułatwienie usług administracji elektronicznej) niż cele, dla których dane były początkowo przetwarzane przez każdą jednostkę administracji publicznej. Powyżsi administratorzy danych, obok innych obowiązków, będą musieli dopilnować, aby system przekazywania danych osobowych od użytkownika do systemu administracji publicznej był bezpieczny, ponieważ w skali makro to przekazywanie danych jest zasadniczym elementem grupy operacji przetwarzania danych przeprowadzonych w ramach portalu.

Inna możliwa struktura − „podejście oparte na pochodzeniu” powstaje, gdy każdy administrator danych jest odpowiedzialny za dane, które wprowadza do systemu. Ma to miejsce w przypadku niektórych ogólnoeuropejskich baz danych, w których kontrola − a tym samym obowiązek działania w oparciu o wnioski o dostęp i sprostowanie − jest powierzana na podstawie krajowego pochodzenia danych osobowych.

Inny interesujący scenariusz jest związany z portalami społecznościowymi.

Przykład nr 12: portale społecznościowe

Dostawcy usługi portalu społecznościowego zapewniają platformy komunikacji online, które umożliwiają osobom publikowanie informacji i wymienianie ich z innymi użytkownikami. Powyżsi dostawcy usług są administratorami danych, ponieważ określają zarówno cele, jak i sposoby przetwarzania takich informacji. Użytkownicy takich portali, zamieszczając dane osobowe również stron trzecich, byliby uznani za administratorów danych, pod warunkiem że ich działania nie są objęte tzw. „wyłączeniem do celów domowych” [17].

Po przeanalizowaniu tych przypadków, w których poszczególne podmioty określają wspólnie jedynie część celów i sposobów przetwarzania danych, bardzo jasno sprecyzowanym i bezproblemowym przypadkiem jest sytuacja, w której wiele podmiotów wspólnie określa i dzieli wszystkie cele i sposoby przetwarzania danych, co prowadzi do pełnoprawnej wspólnej kontroli.

W tym ostatnim przypadku łatwo określić, kto jest właściwy do zapewnienia praw osób, których dane dotyczą, i pełnienia obowiązków z zakresu ochrony danych oraz jest w stanie to uczynić. Zadanie określenia, który administrator jest właściwy − i odpowiedzialny − za jakie prawa i obowiązki osób, których dane dotyczą, jest dużo bardziej złożone, gdy poszczególni wspólni administratorzy danych dzielą wspólne cele i sposoby przetwarzania danych w niesymetryczny sposób.

Konieczność wyraźnego ustalenia podziału kontroli

Po pierwsze, należy zaznaczyć, że szczególnie w przypadku wspólnej kontroli brak możliwości bezpośredniego wywiązania się ze wszystkich obowiązków administratora danych (zapewnienie informacji, prawa dostępu itp.) nie wyklucza możliwości bycia administratorem. Może zdarzyć się, że w praktyce obowiązki te mogłyby być z łatwością pełnione w imieniu administratora danych przez inne strony, które są niekiedy bliżej osób, których dane dotyczą. Administrator danych pozostaje jednak zawsze ostatecznie odpowiedzialny za swoje obowiązki i będzie odpowiadał za ich niewypełnienie.

Zgodnie z poprzednim tekstem przedstawionym przez Komisję w trakcie przyjmowania dyrektywy, posiadanie dostępu do niektórych danych osobowych pociągałoby za sobą fakt bycia (wspólnym) administratorem tych danych. Sformułowanie to nie pojawiło się jednak w wersji ostatecznej, a doświadczenie pokazuje, że sam dostęp do danych nie pociąga za sobą kontroli, natomiast posiadanie dostępu do danych nie jest zasadniczym warunkiem bycia administratorem danych. Dlatego w złożonych systemach obejmujących wiele podmiotów dostęp do danych osobowych i inne prawa osób, których dane dotyczą, mogą być zapewniane na różnych poziomach przez różne podmioty.

Skutki prawne również odnoszą się do odpowiedzialności administratorów danych, w szczególności do kwestii tego, czy „wspólna kontrola” ustanowiona w dyrektywie zawsze pociąga za sobą odpowiedzialność solidarną. W art. 26 dotyczącym odpowiedzialności użyto określenia „administrator danych” w liczbie pojedynczej, wskazując tym samym na odpowiedź twierdzącą. Jak już jednak wspomniano, w rzeczywistości mogą mieć miejsce różne metody działania „wspólnie z”, tj. „wraz z”. W

[17] Więcej szczegółowych informacji i przykładów − zob. opinia grupy roboczej art. 29 5/2009 w sprawie portali społecznościowych przyjęta w dniu 12 czerwca 2009 r. (WP 163).

pewnych okolicznościach może to prowadzić do odpowiedzialności solidarnej, ale nie stanowi to reguły: w wielu przypadkach poszczególni administratorzy danych mogą być odpowiedzialni − a tym samym odpowiadać − za przetwarzanie danych osobowych na różnych etapach i w różnym zakresie.

Efektem końcowym powinno być zapewnienie, nawet w złożonych warunkach przetwarzania danych, w których różni administratorzy danych odgrywają pewną rolę w przetwarzaniu danych osobowych, zgodności z zasadami ochrony danych i wyraźnego przydziału zakresu odpowiedzialności za ewentualne naruszenie tych zasad, aby uniknąć osłabienia ochrony danych osobowych lub powstawania „negatywnego sporu kompetencyjnego" oraz luk, przez co obowiązki lub prawa wynikające z dyrektywy nie są zapewniane przez żadną ze stron.

W takich przypadkach, ważniejsze niż kiedykolwiek jest, by osoby, których dane dotyczą, otrzymały wyraźną informację na temat poszczególnych etapów i podmiotów przetwarzania danych. Ponadto należy wyraźnie określić, czy każdy administrator danych jest właściwy do zapewniania zgodności z wszystkimi prawami osób, których dane dotyczą, albo który administrator danych jest właściwy do którego prawa.

Przykład nr 13: banki i zbiory informacji na temat klientów zalegających z płatnościami

Kilka banków może utworzyć wspólny „zbiór informacji" − o ile prawo krajowe zezwala na takie zbiory − w wyniku czego każdy z nich dostarcza informacje (dane) odnoszące się do klientów zalegających z płatnościami i każdy z banków ma dostęp do wszystkich informacji. Niektóre przepisy stanowią, że wszystkie wnioski osób, których dane dotyczą, na przykład o dostęp do danych lub ich usunięcie, muszą być składane tylko w jednym „punkcie wejścia", u dostawcy. Dostawca jest odpowiedzialny za odnalezienie odpowiedniego administratora danych i zapewnienie należytej odpowiedzi dla osoby, której dane dotyczą. Tożsamość dostawcy jest publikowana w rejestrze przetwarzania danych. W innych systemach prawnych takie zbiory informacji mogą być prowadzone przez oddzielne osoby prawne w roli administratorów, natomiast wnioski o dostęp osób, których dane dotyczą, są przetwarzane przez uczestniczące banki działające jako pośrednicy.

Przykład nr 14: marketing behawioralny

Marketing behawioralny wykorzystuje zgromadzone informacje na temat zachowań użytkowników w zakresie przeglądania stron internetowych, takie jak odwiedzane strony lub wyszukiwania, w celu dobrania do jednostki odpowiedniej reklamy. Zarówno wydawcy, którzy bardzo często wynajmują przestrzeń na stronach internetowych na reklamę, jak i dostawcy sieciowej reklamy, którzy wypełniają tę przestrzeń ukierunkowaną reklamą, mogą gromadzić i wymieniać informacje na temat użytkowników, w zależności od konkretnych warunków umowy.

Z punktu widzenia ochrony danych osobowych wydawcę należy uznać za odrębnego administratora danych, ponieważ gromadzi on dane osobowe od użytkowników (profil użytkownika, adres IP, lokalizacja, język systemu operacyjnego itp.) dla własnych celów. Dostawca reklamy sieciowej będzie również administratorem danych, ponieważ określa on cele (monitorowanie użytkowników na stronach internetowych) lub podstawowe sposoby przetwarzania danych. W zależności od warunków współpracy

pomiędzy wydawcą a dostawcą sieciowej reklamy, jeśli na przykład wydawca umożliwia przekazywanie danych osobowych dostawcy sieciowej reklamy, w tym poprzez przekierowanie użytkownika na stronię internetową dostawcy reklamy sieciowej, mogą oni być wspólnymi administratorami dla grupy operacji przetwarzania danych prowadzących do marketingu behawioralnego.

We wszystkich przypadkach (wspólni) administratorzy danych dbają, by złożoność i szczegóły techniczne systemu behawioralnego marketingu nie stały na przeszkodzie odnalezieniu odpowiednich sposobów wywiązywania się z obowiązków administratora danych i zapewnianiu praw osób, których dane dotyczą. Obejmowałoby to w szczególności:

- *informowanie* użytkownika o tym, że jego dane są dostępne dla strony trzeciej: skuteczniej uczyniłyby to wydawca, który jest głównym partnerem użytkownika.
- oraz o warunkach *dostępu* do danych osobowych: firma zajmująca się reklamą sieciową musiałaby odpowiadać na pytania użytkowników dotyczące sposobu, w jaki prowadzi ukierunkowany marketing wykorzystując dane użytkowników, i musiałaby zastosować się do wniosków o poprawianie i usuwanie danych.

Ponadto wydawca i dostawca reklamy sieciowej mogą podlegać innymi obowiązkom wynikającym z prawa cywilnego i przepisów dotyczących ochrony konsumenta, w tym z prawa deliktów i przepisów dotyczących nieuczciwych praktyk handlowych.

Wstępny wniosek

Strony działające wspólnie mają pewien stopień elastyczności we wzajemnym podziale i przypisywaniu obowiązków i odpowiedzialności, o ile zapewniają pełną zgodność. Zasady dotyczące sposobów ponoszenia wspólnej odpowiedzialności zasadniczo powinny być określone przez administratorów danych. Również w tym przypadku należy uwzględnić faktyczne okoliczności w celu dokonania oceny, czy ustalenia odzwierciedlają rzeczywisty przebieg przetwarzania danych.

W tym kontekście ocena wspólnej kontroli powinna uwzględniać, z jednej strony konieczność zapewnienia pełnej zgodności z przepisami dotyczącymi ochrony danych, a z drugiej strony fakt, że mnożenie administratorów danych może również prowadzić do niepożądanych komplikacji i ewentualnego braku jasności przy przydzielaniu odpowiedzialności. To groziłoby uczynieniem całego przetwarzania nielegalnym ze względu na brak przejrzystości i naruszenie zasady rzetelnego przetwarzania danych.

Przykład nr 15: platformy zarządzania danymi na temat stanu zdrowia

W pewnym państwie członkowskim organ publiczny ustanawia krajowy punkt przejściowy regulujący wymianę danych dotyczących pacjentów między podmiotami służby zdrowia. Olbrzymia liczba administratorów danych − dziesiątki tysięcy − prowadzi do tak niejasnej sytuacji dla osób, których dane dotyczą (pacjentów), że ochrona ich praw jest zagrożona. Dla osób, których dane dotyczą, rzeczywiście nie byłoby jasne, do kogo mogą się zwrócić w razie skarg, pytań i wniosków o informacje, sprostowanie danych osobowych lub dostęp do nich. Ponadto organ publiczny odpowiada za faktyczne zaprojektowanie procesu przetwarzania danych i sposobu jego wykorzystania. Elementy te prowadzą do wniosku, że organ publiczny ustanawiający punkt przejściowy powinien zostać uznany za wspólnego administratora danych oraz za punkt kontaktowy dla wniosków osób, których dane dotyczą.

W związku z powyższym można stwierdzić, że solidarna odpowiedzialność wszystkich zaangażowanych stron powinna zostać uznana za środek eliminujący niepewności, a tym samym przyjęta w założeniu tylko wówczas, gdy alternatywny, jasny i równie skuteczny przydział obowiązków i odpowiedzialności nie został ustanowiony przez zaangażowane strony lub nie wynika jasno z okoliczności faktycznych.

III.2. Definicja przetwarzającego

Pojęcie „przetwarzającego" nie zostało określone w konwencji nr 108. Po raz pierwszy rolę przetwarzającego uznano w pierwszym wniosku Komisji, ale bez wprowadzania tego pojęcia, w celu „uniknięcia sytuacji, w których przetwarzanie danych przez stronę trzecią w imieniu administratora zbioru danych powoduje obniżenie poziomu ochrony, którą jest objęta osoba, której dane dotyczą". Przed uzyskaniem aktualnego sformułowania we wspólnym stanowisku Rady, pojęcie „przetwarzającego" wyrażono w sposób bezpośredni i autonomiczny dopiero w zmienionym wniosku Komisji, a następnie we wniosku Parlamentu Europejskiego.

W taki sam sposób, jak w przypadku definicji „administratora danych", w definicji „przetwarzającego" ujmuje się szeroki zakres podmiotów, które mogą pełnić rolę przetwarzającego („osoba fizyczna lub prawna, władza publiczna, agencja lub inny organ").

Występowanie przetwarzającego zależy od decyzji podjętej przez administratora danych, który może zdecydować o przetwarzaniu danych w ramach własnej organizacji, na przykład, przez pracowników upoważnionych do przetwarzania danych pod jego bezpośrednim zwierzchnictwem (zob. *a contrario* art. 2 lit. f)), lub przekazać całość bądź część działań w zakresie przetwarzania danych organizacji zewnętrznej, tj. – zgodnie z uzasadnieniem do zmienionego wniosku Komisji – „podmiotowi odrębnemu prawnie działającemu w jego imieniu".

W związku z tym dwa podstawowe warunki kwalifikowania się jako przetwarzający to z jednej strony posiadanie statusu osoby prawnej odrębnej od administratora danych, a z drugiej strony przetwarzanie danych osobowych w jego imieniu. Działania w zakresie przetwarzania danych mogą ograniczać się do ściśle określonego zadania lub kontekstu, lub mieć bardziej ogólny charakter i szerszy zakres.

Co więcej, rola przetwarzającego nie wynika z charakteru osoby prawnej przetwarzającej dane, ale z jej konkretnej działalności w określonym kontekście. Innymi słowy, ta sama osoba prawna może działać jednocześnie jako administrator danych w przypadku niektórych operacji przetwarzania danych oraz jako przetwarzający w przypadku innych tego rodzaju operacji, a kwalifikowanie się jako administrator danych lub przetwarzający należy oceniać w odniesieniu do określonych zestawów danych lub operacji.

Przykład nr 16: dostawcy usług internetowych typu hosting

Dostawca usług internetowych typu hosting jest zasadniczo przetwarzającym w przypadku danych osobowych publikowanych online przez jego klientów, na rzecz których świadczy on usługi w zakresie hostingu i prowadzenia strony internetowej. Jeżeli jednak dostawca usług nadal przetwarza do własnych celów dane zawarte na stronach internetowych, jest administratorem danych w odniesieniu do tego określonego działania w zakresie przetwarzania danych. Powyższa analiza różni się od analizy w przypadku dostawcy usług internetowych, takich jak dostęp do poczty elektronicznej lub dostęp do internetu (zob. także przykład nr 1 – dostawcy usług telekomunikacyjnych).

Najważniejszym elementem przepisu jest stwierdzenie, że przetwarzający działa „w imieniu administratora danych". Działanie w czyimś imieniu oznacza działanie w interesie innego podmiotu i przypomina pojęcie prawne „przekazania uprawnień". W przepisach dotyczących ochrony danych wzywa się przetwarzającego do wykonania instrukcji wydanych przez administratora danych, przynajmniej w odniesieniu do celu przetwarzania oraz istotnych elementów lub środków.

Z takiego punktu widzenia zgodność działań przetwarzającego z prawem w zakresie przetwarzania danych jest określona upoważnieniem udzielonym przez administratora danych. Przetwarzający, który wychodzi poza zakres otrzymanego upoważnienia oraz zyskuje znaczącą rolę w określaniu celów lub zasadniczych sposobów przetwarzania, jest (wspólnym) administratorem danych, a nie przetwarzającym. Ocena kwestii zgodności przetwarzania z prawem zostanie jeszcze dokonana w świetle innych artykułów (6–8). Przekazanie uprawnień może wiązać się jednak z pewnym stopniem swobody uznania w odniesieniu do możliwie najlepszego sposobu działania w interesie administratora danych, umożliwiając przetwarzającemu dokonanie wyboru najbardziej odpowiednich środków technicznych i organizacyjnych.

Przykład nr 17: outsourcing usług pocztowych

Podmioty prywatne świadczą usługi pocztowe w imieniu agencji (publicznych) – np. przesyłają przekazem pocztowym zasiłki macierzyńskie i rodzinne w imieniu Krajowej Agencji Zabezpieczenia Społecznego. W takim przypadku organ ochrony danych stwierdził, że przedmiotowe podmioty prywatne należy wyznaczać, jako przetwarzający, biorąc pod uwagę fakt, że ich zadanie - chociaż wykonywane z pewnym stopniem autonomii - zostało ograniczone jedynie do części operacji przetwarzania niezbędnych do realizacji celów określonych przez administratora danych.

Aby zagwarantować, że outsourcing i przekazywanie uprawnień nie spowoduje obniżenia standardu ochrony danych, dyrektywa zawiera także dwa przepisy, które dotyczą w szczególności przetwarzającego i w których w bardzo szczegółowy sposób określa się jego obowiązki w odniesieniu do poufności i bezpieczeństwa.

- Artykuł 16 przewiduje, że sam przetwarzający oraz wszelkie osoby działające z jego upoważnienia, posiadające dostęp do danych osobowych, nie mogą ich przetwarzać bez polecenia administratora danych.

- W odniesieniu do bezpieczeństwa przetwarzania danych art. 17 przewiduje, że stosunki miedzy administratorem danych i przetwarzającym muszą być regulowane umową lub wiążącym aktem prawnym. Umowę sporządza się na piśmie do celów dowodowych oraz ujmuje się w niej podstawowe warunki, przewidujące w szczególności, że przetwarzający działa wyłącznie na polecenie administratora danych i wdraża środki techniczne i organizacyjne umożliwiające odpowiednią ochronę danych osobowych. Umowa powinna zawierać wystarczająco szczegółowy opis upoważnienia przetwarzającego.

W związku z powyższym należy zauważyć, że w wielu przypadkach usługodawcy specjalizujący się w określonych operacjach przetwarzania danych (na przykład, w wypłatach wynagrodzeń) będą określać standardowe usługi oraz umowy do podpisania przez administratorów danych, ustanawiając *de facto* pewien standardowy sposób

przetwarzania danych[18]. Fakt sporządzenia umowy i jej szczegółowych warunków przez usługodawcę, a nie administratora danych nie jest jednak *sam w sobie* wystarczającą podstawą, aby stwierdzić, że należy uznać usługodawcę za administratora danych, ponieważ administrator danych dobrowolnie zaakceptował warunki umowne, tym samym przyjmując za nie pełną odpowiedzialność.

Analogicznie nie należy uznawać nierównowagi w określonych w umowie uprawnieniach małego administratora danych w stosunku do dużego usługodawcy, jako uzasadnienia przyjmowania przez administratora danych klauzul i warunków umów niezgodnych z przepisami dotyczącymi ochrony danych.

Przykład nr 18: platformy poczty elektronicznej

John Smith poszukuje platformy poczty elektronicznej do użytku własnego i pięciu pracowników jego firmy. Dowiaduje się, że odpowiednia i przyjazna dla użytkownika platforma – także jedyna dostępna bezpłatnie – przetrzymuje dane przez zbyt długi okres czasu i przekazuje je do państw trzecich bez właściwych zabezpieczeń. Ponadto nie istnieje możliwość uzgodnienia warunków umownych.

W takim przypadku pan Smith powinien poszukać innego dostawcy lub – w przypadku zarzucanej niezgodności z przepisami dotyczącymi ochrony danych lub braku innych odpowiednich dostawców na rynku – zgłosić sprawę właściwym organom, takim jak organy ochrony danych, organy ds. ochrony konsumentów i konkurencji itp.

Zawarty w dyrektywie wymóg zawarcia umowy na piśmie w celu zapewnienia bezpieczeństwa przetwarzania danych nie oznacza, że administratorzy danych i przetwarzający nie mogą utrzymywać ze sobą stosunków bez wcześniejszego zawarcia umowy. W tym względzie umowa nie ma ani stanowiącego ani rozstrzygającego charakteru, chociaż może pomóc w zrozumieniu stosunków między stronami[19]. W związku z tym także w powyższym przypadku ma zastosowanie podejście funkcjonalne, polegające na analizowaniu rzeczywistych cech stosunków między różnymi podmiotami oraz sposobu określania celów i sposobów przetwarzania danych. W przypadku, jeżeli istnieje stosunek między administratorem danych i przetwarzającym dane, zgodnie z prawem strony te mają obowiązek zawarcia umowy (por. art. 17 dyrektywy).

Wielu przetwarzających dane

Coraz częściej zdarza się, że administrator danych zleca przetwarzanie danych osobowych kilku przetwarzającym. Przetwarzający mogą być bezpośrednio powiązani z administratorem danych lub być podwykonawcami, którym przetwarzający dane przekazał część powierzonych mu działań w zakresie przetwarzania danych.

[18] Opracowywanie warunków przez usługodawcę pozostaje bez uszczerbku dla faktu, że zasadnicze aspekty przetwarzania danych, zgodnie z pkt III.1.b, określa administrator danych.

[19] W niektórych przypadkach jednak zawarcie pisemnej umowy może stanowić warunek konieczny do automatycznego kwalifikowania się jako przetwarzający w określonych sytuacjach. W Hiszpanii, na przykład, w sprawozdaniu na temat centrów obsługi telefonicznej jako przetwarzających określa się wszystkie centra obsługi telefonicznej w państwach trzecich, o ile spełniają warunki umowy. Ma to zastosowanie nawet wówczas gdy umowa została sporządzona przez przetwarzającego, a administrator danych jedynie się do niej „stosuje".

Takie złożone (wielopoziomowe lub rozproszone) struktury przetwarzania danych osobowych stają się coraz bardziej powszechne w związku z nowymi technologiami i niektóre przepisy krajowymi krajowe jednoznacznie do nich nawiązują. Żaden z przepisów dyrektywy nie zabrania tego ze względu na wymogi organizacyjne, jako wykonawców lub podwykonawców przetwarzania danych można wyznaczyć szereg podmiotów, również poprzez podział odnośnych zadań. Przetwarzając dane wszystkie takie podmioty mają jednak obowiązek przestrzegać instrukcji wydanych przez administratora danych.

Przykład nr 19: sieci komputerowe

Duże infrastruktury badawcze coraz częściej wykorzystują rozproszone systemy obliczeniowe, w szczególności przetwarzanie sieciowe, w celu uzyskania korzyści pod względem mocy obliczeniowej i zdolności przechowywania. Sieci instaluje się w różnych infrastrukturach badawczych w różnych krajach. Sieć europejska może na przykład składać się z sieci krajowych, za które z kolei odpowiada organ krajowy. Sieć europejska może jednak nie mieć organu centralnego odpowiedzialnego za jej funkcjonowanie. Badacze korzystający z tej sieci nie są zwykle w stanie ustalić, gdzie dokładnie przetwarza się ich dane, a zatem kto jest odpowiedzialnym przetwarzającym (sprawa staje się jeszcze bardziej skomplikowana, jeżeli infrastruktury gridowe znajdują się w państwach trzecich). Jeżeli infrastruktura gridowa wykorzystuje dane bez zezwolenia, stronę tę można uznać za administratora danych, w przypadku gdy nie działa ona w imieniu badaczy.

W przypadku wielu podmiotów zaangażowanych w proces kwestią strategiczną jest wyraźne przydzielenie zobowiązań i odpowiedzialności wynikających z przepisów dotyczących ochrony danych, tak aby nie były one rozproszone w łańcuchu podwykonawstwa. Innymi słowy, należy unikać łańcucha przetwarzających, który osłabiłby skuteczną kontrolę i jasną odpowiedzialność za działania związane z przetwarzaniem lub nawet je utrudniał, chyba że wyraźnie ustalono obowiązki różnych stron w łańcuchu.

W tym kontekście, analogicznie do pkt III.1.b) – chociaż nie jest konieczne, aby administrator danych określał wszystkie szczegóły dotyczące sposobów wykorzystywanych w dążeniu do zamierzonych celów i zgadzał się na nie – konieczne byłoby co najmniej poinformowanie go o głównych elementach struktury przetwarzania (na przykład zaangażowanych podmiotach, środkach bezpieczeństwa, gwarancjach dotyczących przetwarzania danych w państwach trzecich itd.), tak aby mógł mieć kontrolę nad danymi przetwarzanymi w jego imieniu.

Uznaje się także, że chociaż dyrektywa nakłada na administratora danych odpowiedzialność, nie staje na przeszkodzie, aby krajowe przepisy o ochronie danych stanowiły ponadto, że w niektórych przypadkach odpowiedzialność powinien ponosić przetwarzający.

Niektóre z powyższych kryteriów mogą być pomocne przy określaniu kwalifikacji różnych zaangażowanych podmiotów:

- Poziom wcześniejszych instrukcji wydanych przez administratora danych, który określa margines swobody działania pozostawiony przetwarzającemu;

- Monitorowanie wykonania usługi przez administratora danych. Stały i staranny nadzór sprawowany przez administratora danych w celu zapewnienia pełnej zgodności przetwarzającego z instrukcjami i warunkami umowy wskazuje, że administrator danych nadal sprawuje pełną i wyłączną kontrolę nad operacjami przetwarzania;

- Widoczność/obraz przekazywane przez administratora danych osobie, której dane dotyczą, i oczekiwania osób, których dane dotyczą, na podstawie tej widoczności.

Przykład nr 20: centra telefoniczne (call centre)

Administrator danych zleca część operacji centrum telefonicznemu i poleca mu przedstawienie się, przy wykonywaniu połączeń do klientów administratora danych, wykorzystując tożsamość administratora danych. W tym przypadku oczekiwania klientów i sposób, w jaki administrator danych przedstawia im się za pośrednictwem przedsiębiorstwa outsourcingowego, prowadzą do wniosku, że przedsiębiorstwo outsourcingowe działa jako przetwarzający na rzecz (w imieniu) administratora danych.

- Wiedza ekspercka stron: w niektórych przypadkach dominującą rolę odgrywają tradycyjna rola i wiedza ekspercka dostawcy usług, co może wiązać się z uznaniem go za administratora danych.

Przykład nr 21: adwokaci

Adwokat reprezentuje swojego klienta w sądzie i w związku z tym zadaniem przetwarza dane osobowe związane ze sprawą klienta. Podstawą prawną do wykorzystywania koniecznych informacji jest upoważnienie klienta. Jednak dane upoważnienie nie dotyczy głównie przetwarzania danych, ale reprezentowania w sądzie, do czego zawody te mają tradycyjnie swoją własną podstawę prawną. Zawody takie należy zatem uważać za niezależnych „administratorów danych" w przypadku przetwarzania danych podczas prawomocnego reprezentowania klientów.

W innym kontekście decydująca może być dokładniejsza ocena sposobów zastosowanych, aby osiągnąć cele.

Przykład nr 22: strona internetowa poświęcona rzeczom znalezionym

Stronę poświęconą rzeczom znalezionym przedstawiono jedynie jako przetwarzającego, ponieważ to osoby, które umieszczają informacje o rzeczach zagubionych, określają treść, a zatem jednostkowe cele (np. znalezienie zagubionej broszki, papugi itd.). Organ ochrony danych odrzucił ten argument. Stronę internetową założono w celu biznesowym, jakim jest zarabianie pieniędzy na dopuszczaniu umieszczania informacji o rzeczach zagubionych i fakt, że nie określono, jakie informacje się umieszcza (w odróżnieniu od określenia kategorii rzeczy) nie miał zasadniczego znaczenia, ponieważ definicja „administratora danych" nie obejmuje określania treści. Strona internetowa określa warunki umieszczania informacji itd. i odpowiada za prawidłowość treści.

Chociaż mogła istnieć tendencja do zaliczania outsourcingu do zadań przetwarzającego, obecnie sytuacje i oceny są często znacznie bardziej złożone.

Przykład nr 23: księgowi

Kwalifikacja księgowych może różnić się w zależności od kontekstu. W przypadku gdy księgowi świadczą usługi na rzecz społeczeństwa i drobnych przedsiębiorców na podstawie bardzo ogólnych instrukcji („Proszę przygotować moją deklarację podatkową"), tak jak obrońcy działający w podobnych okolicznościach i z podobnych powodów, księgowy będzie administratorem danych. Jednak jeżeli przedsiębiorstwo to zatrudnia księgowego i wypełnia on szczegółowe polecenia wewnętrznego księgowego, być może dotyczące przeprowadzenia szczegółowego audytu, wówczas, jeżeli księgowy nie jest stałym pracownikiem, będzie on zazwyczaj przetwarzającym w związku z jasnością poleceń, a w ich następstwie ograniczonym zakresem swobody. Podlega to jednak istotnemu zastrzeżeniu, mianowicie jeżeli księgowi uważają, że wykryli nieuczciwe działania, które są zobowiązani zgłosić, wtedy z powodu zobowiązań zawodowych działają niezależnie jako administratorzy danych.

Niekiedy złożoność operacji przetwarzania może prowadzić do położenia większego nacisku na margines swobody działania osób, którym powierzono przetwarzanie danych osobowych, np. jeżeli przetwarzanie wiąże się z konkretnym ryzykiem dla prywatności. Wprowadzenie nowych sposobów przetwarzania może prowadzić do sprzyjania uznawaniu za administratora danych, a nie przetwarzający dane. Przypadki te mogą również doprowadzić do wyjaśnienia i wyznaczenia administratora danych przewidzianego jednoznacznie w przepisach prawa.

Przykład nr 24: przetwarzanie dla celów historycznych, naukowych i statystycznych

W odniesieniu do przetwarzania danych osobowych dla celów historycznych, naukowych i statystycznych przepisy krajowe mogą wprowadzić pojęcie organizacji pośredniczącej w celu wyznaczania organu odpowiadającego za przekształcanie danych niekodowanych w dane kodowane, tak aby administrator danych przetwarzanych dla celów historycznych, naukowych i statystycznych nie mógł ponownie zidentyfikować osób, których dane dotyczą.

Jeżeli kilku administratorów operacji wstępnego przetwarzania przekazuje dane co najmniej jednej osobie trzeciej, aby przetwarzała je dla celów historycznych, naukowych i statystycznych, dane koduje najpierw organizacja pośrednicząca. W tym przypadku organizację pośredniczącą można uważać za administratora danych zgodnie z konkretnymi przepisami krajowymi i podlega ona wszystkim wynikającym z nich zobowiązaniom (adekwatność danych, informowanie osoby, której dane dotyczą, powiadamianie itd.). Jest to uzasadnione tym, że w przypadku gromadzenia danych z różnych źródeł występuje szczególne zagrożenie dla ochrony danych, uzasadniające własną odpowiedzialność organizacji pośredniczącej. W rezultacie nie uznaje się jej po prostu za przetwarzającego, ale w pełni za administratora danych zgodnie z przepisami krajowymi.

Analogicznie istotne są autonomiczne uprawnienia do podejmowania decyzji pozostawione różnym stronom zaangażowanym w przetwarzanie. Przypadek badań klinicznych leków pokazuje, że związek między przedsiębiorstwami finansującymi i podmiotami zewnętrznymi, którym powierzono prowadzenie badań, zależy od

pozostawionej podmiotom zewnętrznym swobody w zakresie przetwarzania danych. Wiąże się to z możliwością istnienia więcej niż jednego administratora danych, ale także większej liczby przetwarzających lub osób odpowiedzialnych za przetwarzanie.

Przykład nr 25: badania kliniczne leków

Przedsiębiorstwo farmaceutyczne XYZ finansuje pewne badania leków i wybiera kandydujące ośrodki badań, oceniając kwalifikowalność i interesy każdego z nich; sporządza protokół badania, dostarcza centrom niezbędne wytyczne w odniesieniu do przetwarzania danych i sprawdza zgodność centrów zarówno z protokołem, jak i z odpowiednimi procedurami wewnętrznymi.

Chociaż sponsor nie zbiera żadnych danych bezpośrednio, wchodzi w posiadanie danych dotyczących pacjentów, zgromadzonych przez ośrodki badań i przetwarza te dane w różny sposób (ocena informacji zawartych w dokumentacji medycznej; otrzymywanie danych na temat niepożądanych reakcji; wprowadzanie tych danych do odpowiedniej bazy danych; prowadzenie analiz technicznych w celu otrzymania wyników badań). Ośrodek badań prowadzi badania w sposób autonomiczny, jednak zgodnie z wytycznymi sponsora; dostarcza pacjentom zawiadomienia i otrzymuje ich zgodę także na przetwarzanie dotyczących ich danych; zapewnia współpracownikom sponsora dostęp do oryginalnej dokumentacji medycznej pacjentów w celu przeprowadzenia działań kontrolnych, a także zajmuje się bezpiecznym przechowywaniem tych dokumentów i odpowiada za nie. Wydaje się zatem, że odpowiedzialność powierzana jest pojedynczym podmiotom.

W tym kontekście w danym przypadku zarówno ośrodki badań, jak i sponsorzy decydują w znaczący sposób o przetwarzaniu danych osobowych odnoszących się do badań klinicznych. W związku z tym można uważać ich za wspólnych administratorów danych. Związek między sponsorem i ośrodkami badań można interpretować inaczej w przypadkach, gdy sponsor określa cele i zasadnicze elementy sposobów, a badaczowi pozostawiono bardzo wąski margines działania swobody działania.

III.3. Definicja osoby trzeciej

Pojęcie „osoby trzeciej” nie zostało określone w konwencji nr 108, ale wprowadzono je wnioskiem Komisji zmienionym zgodnie z poprawką zaproponowaną przez Parlament Europejski. Zgodnie z uzasadnieniem zmiana została przeredagowana w celu wyjaśnienia, że osoby trzecie nie obejmują osoby, której dotyczą dane, administratora danych ani żadnej osoby upoważnionej do przetwarzania danych pod bezpośrednim zwierzchnictwem administratora danych lub w jego imieniu, jak w przypadku przetwarzającego. Oznacza to, że „osoby pracujące dla innej organizacji, nawet jeżeli należy ona do tej samej grupy lub spółki dominującej, zasadniczo są osobami trzecimi”, natomiast z drugiej strony „oddziały banku przetwarzające dane dotyczące rachunków klientów pod bezpośrednim nadzorem ich siedziby głównej, nie będą osobami trzecimi”.

W dyrektywie stosuje się pojęcie „osoby trzeciej” w sposób nieróżniący się od sposobu, w jaki pojęcie to jest zwykle stosowane w prawie cywilnym, w którym osoba trzecia jest zazwyczaj podmiotem, który nie jest częścią innego podmiotu ani stroną umowy. W kontekście ochrony danych pojęcie to powinno być interpretowane jako odnoszące się do każdego podmiotu, który nie ma żadnego konkretnego umocowania prawnego ani

upoważnienia do przetwarzania danych osobowych, które mogłoby wynikać np. z jego funkcji jako administratora danych, przetwarzającego lub ich pracownika.

W dyrektywie stosuje się to pojęcie w różnych przepisach, zazwyczaj w celu ustanowienia zakazów, ograniczeń i obowiązków w przypadkach, w których dane osobowe mogą być przetwarzane przez inne osoby, które nie zostały wyznaczone do przetwarzania pewnych danych osobowych.

Na podstawie tych informacji można stwierdzić, że osoba trzecia otrzymująca dane osobowe – zgodnie lub niezgodnie z prawem – w zasadzie stanowi nowego administratora danych, pod warunkiem że spełnione zostaną inne warunki zakwalifikowania tej osoby jako administratora danych i stosowania przepisów dotyczących ochrony danych.

Przykład nr 26: nieupoważniony dostęp pracownika

Podczas wykonywania swoich zadań pracownik przedsiębiorstwa poznaje dane osobowe, do dostępu do których nie jest upoważniony. W tym przypadku pracownika tego powinno się uznać za „osobę trzecią" w stosunku do pracodawcy, ze wszystkimi wynikającymi z tego konsekwencjami i odpowiedzialnością w zakresie legalności przekazywania i przetwarzania danych.

IV. Wnioski

Pojęcie administratora danych i jego interakcja z pojęciem przetwarzającego odgrywają zasadniczą rolę w stosowaniu dyrektywy 95/46/WE, ponieważ określają, kto odpowiada za zgodność z zasadami ochrony danych, w jaki sposób osoby, których dotyczą dane, mogą wykonywać swoje prawa, jakie prawo krajowe ma zastosowanie i jak skutecznie mogą działać organy ochrony danych.

Zróżnicowanie organizacyjne zarówno sektora publicznego, jak i prywatnego, rozwój TIK oraz globalizacja przetwarzania danych zwiększają złożoność sposobu przetwarzania danych osobowych i wiążą się z koniecznością wyjaśnienia omawianych pojęć w celu zapewnienia ich skutecznego stosowania i zgodności w praktyce.

Pojęcie administratora danych jest autonomiczne, w tym znaczeniu, że należy je interpretować głównie według wspólnotowych przepisów o ochronie danych, i funkcjonalne w tym znaczeniu, że ma na celu przydzielanie zadań tam, gdzie występuje faktyczny wpływ, a zatem opiera się raczej na analizie okoliczności faktycznych niż na analizie formalnej.

Definicja zamieszczona w dyrektywie składa się z trzech głównych modułów: aspektów o charakterze personalnym („osoba fizyczna lub prawna, władza publiczna, agencja lub inny organ"); możliwości kontroli pluralistycznej („który samodzielnie lub wspólnie z innymi podmiotami"); oraz zasadniczych elementów odróżniających administratora danych od innych podmiotów („określa cele i sposoby przetwarzania danych").

Analiza tych elementów składowych prowadzi do następujących głównych wniosków:

- Zdolność, zgodnie z którą „*określa* cele i sposoby...", może wynikać z różnych okoliczności prawnych lub faktycznych: z jednoznacznych właściwości prawnych, jeżeli przepisy prawa mianują administratora danych, przyznają mu zadanie lub nakładają na niego obowiązek gromadzenia i przetwarzania danych; ze wspólnych przepisów prawnych lub tradycyjnych ról, które zwykle oznaczają pewną odpowiedzialność w niektórych organizacjach (np. pracodawcy w odniesieniu do danych dotyczących jego pracowników); z okoliczności faktycznych i innych elementów (takich jak stosunki umowne, faktyczna kontrola przez stronę, przejrzystość w stosunku do podmiotów, których dotyczą dane itd.).

  Jeżeli żadna z wyżej wymienionych kategorii nie znajdzie zastosowania, mianowanie administratora danych należy uważać za nieważne. Organu, który nie ma prawnego ani faktycznego wpływu na sposób przetwarzania danych osobowych, nie można uważać za administratora danych.

  Określenie „celu" przetwarzania powoduje uznanie za administratora danych (*de facto*). Administrator danych może natomiast przekazać określenie „sposobów" przetwarzania w odniesieniu do kwestii technicznych i organizacyjnych. Określenie zasadniczych kwestii dotyczących sedna zgodności przetwarzania danych z prawem – takich jak dane, które należy przetworzyć, czas ich przechowywania, dostęp do nich itd. – należy do administratora danych.

- Zawarte w definicji aspekty *o charakterze personalnym* odnoszą się do obszernej grupy podmiotów, które mogą pełnić funkcję administratora danych. W strategicznym kontekście przydzielania obowiązków w pierwszej kolejności należy za administratora danych uznać przedsiębiorstwo jako takie lub organ jako taki, a nie szczególną osobę w przedsiębiorstwie lub organie. To właśnie przedsiębiorstwo lub organ ostatecznie uznaje się za odpowiedzialne za przetwarzanie danych i pełnienie obowiązków wynikających z przepisów dotyczących ochrony danych, chyba że istnieją wyraźne elementy wskazujące na to, że odpowiedzialna jest osoba fizyczna, np. jeżeli osoba fizyczna pracująca w przedsiębiorstwie lub dla podmiotu prawa publicznego wykorzystuje dane do własnych celów nieobjętych zakresem działalności przedsiębiorstwa.

- Możliwość *kontroli pluralistycznej* przewiduje rosnącą liczbę sytuacji, w których różne strony działają jako administratorzy danych. Ocena wspólnej kontroli powinna odzwierciedlać ocenę „pojedynczej" kontroli poprzez przyjęcie konkretnego i funkcjonalnego podejścia, a także koncentrując się na tym, czy cele i zasadnicze elementy sposobów są określane przez więcej stron niż jedną.

  Udział stron w określaniu celów i sposobów przetwarzania w kontekście wspólnej kontroli może przyjmować różne formy i nie musi być jednakowy. Niniejsza opinia zawiera wiele przykładów różnych typów i stopni wspólnej kontroli. Z różnych stopni kontroli mogą wynikać różne stopnie odpowiedzialności i zobowiązań, a solidarnej odpowiedzialności nie można na pewno założyć we wszystkich przypadkach. Ponadto bardzo możliwe jest, że w złożonych systemach z wieloma podmiotami dostęp do danych osobowych i wykonywanie innych praw osób, których dotyczą dane, mogą być zapewnione również na różnych poziomach przez różne podmioty.

W niniejszej opinii przeprowadzono również analizę pojęcia przetwarzającego. Jego istnienie zależy od decyzji podjętej przez administratora danych, który może podjąć decyzję o przetwarzaniu danych w swojej organizacji lub o przekazaniu organizacji zewnętrznej całości bądź części działań związanych z przetwarzaniem. W związku z tym podmiot może być przetwarzającym, jeżeli spełnia dwa podstawowe warunki: po pierwsze, jest odrębną osobą prawną w stosunku do administratora danych, pod drugie, przetwarza dane osobowe w jego imieniu. Działania związane z przetwarzaniem mogą się ograniczać do bardzo szczególnego zadania lub kontekstu lub mogą wiązać się z pewnym stopniem swobody uznania w odniesieniu do możliwie najlepszego sposobu działania w interesie administratora danych, umożliwiając przetwarzającemu dokonanie wyboru najbardziej odpowiednich środków technicznych i organizacyjnych.

Co więcej, rola przetwarzającego nie wynika z jego charakteru, ale z konkretnej działalności w określonym kontekście oraz w związku z określonymi zestawami danych lub grupami operacji. Niektóre kryteria mogą być pomocne w określeniu kwalifikacji różnych podmiotów zaangażowanych w przetwarzanie: poziom uprzedniego polecenia wydanego przez administratora danych; monitorowanie poziomu usługi przez administratora danych; przejrzystość w stosunku do podmiotów, których dotyczą dane; wiedza ekspercka stron; autonomiczne uprawnienia do podejmowania decyzji pozostawione różnym stronom.

Kategoria „osoby trzeciej" jest określana jako każdy podmiot, który nie ma żadnej szczególnej zasadności ani upoważnienia – jakie mogłoby wynikać np. z jego funkcji jako administratora danych, przetwarzającego lub ich pracownika – do przetwarzania danych osobowych.

* * *

Grupa robocza dostrzega trudności w stosowaniu definicji użytych do celów dyrektywy w złożonych okolicznościach, w których można przewidzieć wiele scenariuszy samodzielnego lub wspólnego funkcjonowania administratorów danych i przetwarzających, przy różnym stopniu autonomii i odpowiedzialności.

W swojej analizie grupa robocza podkreśliła potrzebę przydzielenia odpowiedzialności w taki sposób, aby zapewnić w praktyce wystarczającą zgodność z zasadami ochrony danych. Nie znalazła jednak powodów, aby przypuszczać, że obecne rozróżnienie między administratorami danych i przetwarzającymi nie będzie już w tej perspektywie odpowiednie i użyteczne.

Grupa robocza ma zatem nadzieję, że przedstawione w niniejszej opinii wyjaśnienia, zilustrowane konkretnymi przykładami zaczerpniętymi z codziennych doświadczeń organów ochrony danych, pomogą w interpretacji tych podstawowych definicji użytych do celów dyrektywy.

Sporządzono w Brukseli dnia 16 lutego 2010 r.

W imieniu grupy roboczej
Przewodniczący
Jacob KOHNSTAMM