



00658/13/PL
WP 204

Dokument wyjaśniający w sprawie wiążących reguł korporacyjnych przetwarzającego

przyjęty w dniu 19 kwietnia 2013 r.

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

Obsługę sekretariatu zapewnia Dyrekcja C (Prawa Podstawowe i Obywatelstwo Unii Europejskiej) Dyrekcji Generalnej ds. Sprawiedliwości Komisji Europejskiej, B-1049 Bruksela, Belgia, Biuro nr MO-59 02/013.

Strona internetowa: http://ec.europa.eu/justice/data-protection/index_en.htm

SPIS TREŚCI

strona

. KONTEKST	4
1.1. Reguły Unii Europejskiej dotyczące międzynarodowego przekazywania danych	4
1.2. Wiążące reguły korporacyjne dla administratorów danych	4
1.3. Wiążące reguły korporacyjne dla przetwarzających	5
2. DEFINICJA I KWESTIE PRAWNE.....	6
2.1. Zakres przedmiotowego instrumentu i definicje	6
2.2. Przekazywanie danych i dalsze przekazywanie danych.....	7
2.2.1. Przekazywanie danych w ramach grupy przetwarzającego	7
2.2.2. Dalsze przekazywanie danych do zewnętrznych podprzetwarzających	8
2.3. Postanowienia dotyczące wiążącego charakteru wiążących reguł korporacyjnych dla przetwarzających	8
2.3.1. Wiążący charakter reguł korporacyjnych dla przetwarzających w ramach organizacji.....	9
2.3.2. Wiążący charakter reguł korporacyjnych dla przetwarzających w odniesieniu do zewnętrznych podmiotów podprzetwarzających dane.....	10
2.3.3. Możliwość prawnego egzekwowania reguł korporacyjnych	10
2.3.4. Obowiązkowe wymagania ustawodawstwa krajowego mające zastosowanie do członków organizacji	13
3. ZAWARTOŚĆ MERYTORYCZNA WIĄŻĄCYCH REGUŁ KORPORACYJNYCH DLA PRZETWARZAJĄCYCH	14
3.1. Zawartość merytoryczna i poziom szczegółowości	14
3.2. Aktualizacja wiążących reguł korporacyjnych.....	15
4. ZAPEWNIENIE ZGODNOŚCI I GWARANCJA EGZEKWOWANIA	15
4.1. Przepisy gwarantujące istotny poziom zgodności	16
4.2. Audyty	16
4.3. Rozpatrywanie skarg	17
4.4. Obowiązek współpracy z administratorem danych	18

4.5.	Obowiązek współpracy z organami ochrony danych	18
4.6.	Odpowiedzialność	19
4.6.1.	Ogólne prawo do otrzymania zadośćuczynienia oraz stosownego odszkodowania.....	19
4.6.2.	Reguły dotyczące odpowiedzialności	19
4.7.	Reguła dotycząca jurysdykcji	21
4.8.	Przejrzystość	21
5.	WNIOSEK	22

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.¹,

uwzględniając art. 29 oraz art. 30 ust. 1 lit. a) i ust. 3 tej dyrektywy,

uwzględniając swój regulamin wewnętrzny, w szczególności jego art. 12 i 14,

PRZYJMUJE NINIEJSZY DOKUMENT ROBOCZY:

1. KONTEKST

1.1. Reguły Unii Europejskiej dotyczące międzynarodowego przekazywania danych

Zgodnie z dyrektywą przekazywanie danych poza Unię Europejską musi podlegać ścisłym uregulowaniom, aby zapewnić osobom, których dane dotyczą, odpowiedni stopień ochrony, nawet gdy ich dane przesyłane są poza Unię Europejską (zwaną dalej „UE”).

Art. 26 ust. 2 dyrektywy stanowi, że „(...) Państwo Członkowskie może zezwolić na przekazanie lub przekazywanie danych osobowych do państwa trzeciego, które nie zapewnia odpowiedniego stopnia ochrony (...), jeżeli administrator danych zaleci odpowiednie zabezpieczenia odnośnie do ochrony prywatności oraz podstawowych praw i wolności osoby oraz odnośnie do wykonywania odpowiednich praw; takie środki zabezpieczające mogą w szczególności wynikać z odpowiednich klauzul umownych.”.

W związku z tym, gdy państwo importera danych nie zapewnia odpowiedniego stopnia ochrony, administrator danych musi zapewnić wystarczające gwarancje w odniesieniu do przekazywanych danych, na przykład poprzez przyjęcie klauzul umownych.

Na tej podstawie oraz w celu ułatwienia zachowania zgodności przekazywania danych poza UE z dyrektywą 95/46 Komisja Europejska przyjęła zestawy standardowych klauzul umownych – 2001/497/WE z dnia 15 czerwca 2001 r. i 2004/915/WE z dnia 27 grudnia 2004 r. w odniesieniu do przekazywania danych między administratorami danych oraz 2010/87/UE z dnia 5 lutego 2010 r. w odniesieniu do przekazywania danych między administratorami danych i przetwarzającymi.

1.2. Wiążące reguły korporacyjne dla administratorów danych

Mając świadomość potrzeby stosowania przez organizacje globalnego podejścia w odniesieniu do ochrony danych, Grupa Robocza Art. 29 uznała za konieczne nadanie organizacjom uprawnień do przyjmowania wiążących zasad wewnętrznych, tzw. wiążących reguł korporacyjnych, których celem jest uregulowanie przekazywania danych osobowych przetwarzanych pierwotnie przez organizację jako administratora danych w ramach tej samej

¹ Dziennik Urzędowy nr L 281 z 23.11.1995, s. 31, dostępna na stronie internetowej: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:pl:HTML>.

organizacji. Organy ochrony danych UE opracowały „zestaw narzędzi” zapewniający wytyczne na temat oczekiwań w stosunku do zawartości wiążących reguł korporacyjnych².

Poza tym należy zauważyć, że chociaż standardowe klauzule umowne są rozwiązaniem „nieszablonyowym”, każdy zestaw wiążących reguł korporacyjnych musi być dostosowany do szczególnych potrzeb danego przedsiębiorstwa. Ponadto chociaż standardowe klauzule umowne zwykle podpisywane są bez potrzeby jakiegokolwiek szczególnego wdrażania, podstawą wiążących reguł korporacyjnych jest organizacja, która posiada wystarczająco zadowalający i solidny system ochrony danych, funkcjonujący już w ramach grupy, lub która wprowadza niezbędne środki w celu zapewnienia spełnienia wymogów określonych w wiążących regułach korporacyjnych przez funkcjonujące systemy.

W ciągu ostatnich kilku lat wiążące reguły korporacyjne dla administratorów danych okazały się coraz bardziej skuteczne. Długość procedury przyjmowania została istotnie ograniczona nie tylko dzięki rosnącemu doświadczeniu organów ochrony danych i organizacji, lecz także dzięki procedurze wzajemnego uznawania. Ponadto organizacje wielonarodowe nieustannie potwierdzały, że wiążące reguły korporacyjne są dostosowane do pragmatycznego podejścia, które organizacje te usiłują stosować w odniesieniu do kwestii zgodności. Dodatkowo Komisja Europejska udzieliła wsparcia na rzecz wiążących reguł korporacyjnych poprzez włączenie ich do projektu rozporządzenia w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych opublikowanego dnia 25 stycznia 2012 r.³.

1.3. Wiążące reguły korporacyjne dla przetwarzających

W 2010 r. Komisja Europejska przyjęła nowy zestaw standardowych klauzul umownych w odniesieniu do przekazywania danych między administratorami danych i przetwarzającymi w odpowiedzi na rozwój działalności związanej z przetwarzaniem oraz w szczególności na pojawienie się nowych modeli biznesowych w zakresie międzynarodowego przetwarzania danych osobowych. Standardowe klauzule umowne z 2010 r. zawierają szczególne przepisy, które na pewnych warunkach pozwalają na outsourcing działalności związanej z przetwarzaniem podmiotom podprzetwarzającym, a tym samym zapewniają wystarczające gwarancje w zakresie przekazywanych danych osobowych.

Gwarantowanie w sposób ciągły odpowiedniego stopnia ochrony z zastosowaniem dostępnych narzędzi służących do opisanego wyżej uregulowania międzynarodowego przekazywania danych staje się coraz trudniejsze, głównie ze względu na fakt rosnącej liczby i złożoności przypadków przekazywania (co wynika np. z przetwarzania danych w chmurze obliczeniowej, globalizacji, powstania centrów danych, sieci społecznościowych itd.).

Chociaż wydaje się, że standardowe klauzule umowne są skuteczne do celów uregulowania niemasowego przekazywania danych przez eksportera danych zlokalizowanego w UE do importera danych zlokalizowanego poza UE, branża outsourcingowa nieustannie domaga się nowych instrumentów prawnych, które pozwalałyby na stosowanie globalnego podejścia do

² Zob. WP153, WP154 i WP155 http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/tools/index_en.htm.

³ Zob. art. 42 projektu rozporządzenia w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_pl.pdf.

ochrony danych w działalności outsourcingowej oraz oficjalnie uznaje zasady wewnętrzne wdrożone przez organizacje. Taki nowy instrument prawny mógłby okazać się efektywny do celów uregulowania przekazywania danych przez przetwarzających do podprzetwarzających należących do tej samej organizacji, działających w imieniu i zgodnie z instrukcjami administratora danych. Biorąc pod uwagę rosnące zainteresowanie sektora takim narzędziem, Grupa Robocza Art. 29 przyjęła w 2012 r. dokument roboczy, w którym zawarła tabelę przedstawiającą elementy i zasady, które powinny znaleźć się w wiążących regułach korporacyjnych dla przetwarzających⁴, oraz formularz zgłoszeniowy służący do zgłaszania wiążących reguł korporacyjnych dla przetwarzających⁵. Dnia 5 grudnia 2012 r. Grupa Robocza Art. 29 potwierdziła wprowadzenie wiążących reguł korporacyjnych dla przetwarzających⁶.

2. DEFINICJA I KWESTIE PRAWNE

2.1. Zakres przedmiotowego instrumentu i definicje

Wiążące reguły korporacyjne dla przetwarzających zostały opracowane jako narzędzie, które mogłoby pomóc w uregulowaniu międzynarodowego przekazywania danych osobowych pierwotnie przetwarzanych przez przetwarzającego w imieniu i zgodnie z instrukcjami⁷ administratora danych w UE oraz podprzetwarzanych w ramach organizacji przetwarzającego.

W związku z tym wiążące reguły korporacyjne dla przetwarzających są załączane do umowy przetwarzającego (zwanej w niniejszym dokumencie umową o gwarantowanym poziomie usług), która jest wymagana zgodnie z art. 17 dyrektywy 95/46/WE i zawiera w szczególności instrukcje administratora danych podpisane między zewnętrznym administratorem danych i przetwarzającym. Wiążące reguły korporacyjne dla przetwarzających należy rozumieć jako odpowiednie zabezpieczenia zapewniane przez przetwarzającego na rzecz administratora danych (art. 26 ust. 2 dyrektywy UE 95/46), które pozwala administratorowi danych zapewnić zgodność z mającymi zastosowanie przepisami UE w zakresie ochrony danych. Jednostki grupy przetwarzającego zobowiązują się do przestrzegania zasad zawartych w wiążących regułach korporacyjnych dla przetwarzających i ponoszą odpowiedzialność przed administratorem danych w przypadku naruszenia wiążących reguł korporacyjnych dla przetwarzających.

Należy jednak podkreślić fakt, że chociaż organy ochrony danych UE oceniają treść wiążących reguł korporacyjnych dla przetwarzających należących do grupy przetwarzającego w celu zapewnienia spełnienia wszystkich wymogów określonych w WP195, administrator danych pozostaje odpowiedzialny za zapewnienie wystarczających gwarancji w odniesieniu

⁴ Zob. WP195, przyjęty dnia 6 czerwca 2012 r., http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf.

⁵ Zob. formularz zgłoszeniowy służący do zatwierdzenia wiążących reguł korporacyjnych dotyczących przekazywania danych osobowych do celów działalności związanej z przetwarzaniem, przyjęty dnia 17 września 2012 r., http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_application_form_en.doc.

⁶ Zob. komunikat prasowy ogłoszony dnia 21 grudnia 2012 r., http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20121221_pr_bcrs_en.pdf.

⁷ Administrator danych osoby trzeciej wezwany przez przedsiębiorstwo outsourcingowe, które będzie dokonywało międzynarodowego przekazywania danych do jednostek swojej grupy przedsiębiorstw występujących jako podprzetwarzający.

do danych przekazywanych i przetwarzanych w jego imieniu i zgodnie z jego instrukcjami w jednostkach grupy przetwarzającego.

Grupa Robocza Art. 29 przypomina, że celem wiążących reguł korporacyjnych dla przetwarzających nie jest przeniesienie obowiązków administratorów danych na przetwarzających. Obowiązki przetwarzających i administratorów danych w kontekście międzynarodowego przekazywania danych nie ulegają zmianie (analogicznie do standardowych klauzul umownych 2010/87/UE), jednak niektóre narzędzia będą musiały zostać dostosowane do szczególnych cech przekazywania danych w ramach tej samej grupy organizacji (jedno globalne zobowiązanie zamiast szeregu umów) oraz do szczególnych cech wiążących reguł korporacyjnych (narzędzi rozliczalności takich jak kontrola, programy szkoleniowe, urzędnicy ds. ochrony danych itd.).

Ponadto wiążące reguły korporacyjne dla przetwarzających powinny wzmacniać prawa osób, których dane dotyczą, poprzez wyraźne zapewnienie zobowiązania się przetwarzających do dostarczania administratorom danych odpowiednich informacji umożliwiających im wypełnianie ich obowiązków w odniesieniu do osób, których dane dotyczą. Wydaje się, że wiążące reguły korporacyjne dla przetwarzających stanowią dodatkową gwarancję, że przetwarzający będą dostarczać administratorom danych odpowiednie informacje.

Ponadto przetwarzający będzie musiał ubiegać się o uznanie przez UE jego reguł korporacyjnych dla przetwarzających za odpowiednie zabezpieczenia w odniesieniu do międzynarodowego przekazywania danych zgodnie z procedurą wzajemnego uznawania i procedurą współpracy, które określono w WP107⁸, natomiast administratorzy danych nadal będą musieli ubiegać się o krajowe zezwolenia u właściwych organów ochrony danych na przekazywanie danych do różnych jednostek swoich usługodawców (przetwarzających, podprzetwarzających, centrów danych itd.) na podstawie wiążących reguł korporacyjnych dla przetwarzających będących częścią gwarancji zapewnianych przez administratorów danych.

2.2. Przekazywanie danych i dalsze przekazywanie danych

2.2.1. Przekazywanie danych w ramach grupy przetwarzającego

Biorąc pod uwagę, że zgodnie z WP195 dane mogą być podprzetwarzane przez innych członków grupy przetwarzającego wyłącznie po uprzednim poinformowaniu administratora danych⁹ i wydaniu przez niego uprzedniej zgody na piśmie, wiążące reguły korporacyjne dla przetwarzających zapewniają przejrzystość w odniesieniu do administratora danych i pozostawiają mu kontrolę nad danymi przetwarzanymi przez jednostki grupy przetwarzającego w jego imieniu i zgodnie z jego instrukcjami.

Strony umowy o gwarantowanym poziomie usług mają swobodę decydowania, w zależności od swoich indywidualnych potrzeb, o tym, czy ogólna uprzednia zgoda wydana przez administratora danych na początku świadczenia usługi jest wystarczająca, czy też wymagana jest szczególna zgoda administratora danych w odniesieniu do każdego nowego podprzetwarzania. W przypadku wydania zgody ogólnej administrator danych powinien

⁸ Zob. WP107, przyjęty dnia 14 kwietnia 2005 r., http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp107_en.pdf.

⁹ Chodzi o informacje dotyczące głównych elementów (stron, państw, bezpieczeństwa, gwarancji w przypadku międzynarodowego przekazywania danych, z możliwością uzyskania kopii zastosowanych umów). Szczegółowe informacje dotyczące np. nazwy podprzetwarzających można uzyskać na przykład w publicznym rejestrze elektronicznym.

zostać poinformowany o wszelkich zamierzonych zmianach dotyczących wyboru dodatkowego podwykonawcy lub jego zastąpienia z takim wyprzedzeniem czasowym, które pozwoli administratorowi danych na zakwestionowanie zmiany lub wypowiedzenie umowy, zanim dane zostaną przekazane nowemu podprzetwarzającemu.

Organizacja przetwarzającego, która wdrożyła wiążące reguły korporacyjne dla przetwarzających, nie będzie musiała podpisywać umów w celu uregulowania przekazywania danych z każdym wchodzącym w jej skład podmiotem podprzetwarzającym, ponieważ w odniesieniu do wiążących reguł korporacyjnych dla przetwarzających zapewniane są zabezpieczenia w zakresie przekazywania i przetwarzania danych w imieniu i zgodnie z instrukcjami administratora danych.

2.2.2. Dalsze przekazywanie danych do zewnętrznych podprzetwarzających

Poza zasadami określonymi powyżej w odniesieniu do przekazywania danych w ramach grupy przetwarzającego (przejrzystość, zgoda administratora danych) członek grupy przetwarzającego może zlecać podwykonawstwo swoich obowiązków zgodnie z umową o gwarantowanym poziomie usług (art. 17 dyrektywy) zewnętrznemu podprzetwarzającemu (spoza grupy) wyłącznie na podstawie pisemnej umowy zawartej z zewnętrznym podprzetwarzającym, która zapewnia odpowiednią ochronę zgodnie z art. 16 i 17 dyrektywy 95/46/WE oraz zapewnia przestrzeganie przez zewnętrznych podprzetwarzających tych samych obowiązków, jakie ciążą na członkach grupy przetwarzającego zgodnie z umową o świadczenie usług oraz sekcjami 1.3, 1.4, 3 i 6 dokumentu roboczego 195¹⁰. Ponadto w zakresie, w jakim wiążące reguły korporacyjne dla przetwarzających nie mają zastosowania do przekazywania danych do zewnętrznych podprzetwarzających (spoza grupy), odpowiednia ochrona w odniesieniu do wspomnianego przekazywania danych zapewniana jest zgodnie z art. 25 i 26 dyrektywy 95/46/WE.

2.3. Postanowienia dotyczące wiążącego charakteru wiążących reguł korporacyjnych dla przetwarzających

Przetwarzający reagują na potrzeby w zakresie działań dotyczących przetwarzania danych w oparciu o różne uwarunkowania prawne i kulturowe oraz różne zasady i praktyki biznesowe. Doświadczenia związane z wiążącymi regułami korporacyjnymi dla administratorów danych wskazują wyraźnie, że prawie każda organizacja wielonarodowa podchodzi do tej kwestii w odmienny sposób. Istnieje jednak m.in. istotny element, który musi być obecny we wszystkich systemach, jeżeli mają być one stosowane w celu zapewniania zabezpieczeń w zakresie przekazywania danych państwom trzecim do celów działalności związanej z przetwarzaniem: tj. wiążący charakter reguł korporacyjnych dla przetwarzających, zarówno wewnętrznie, jak i w odniesieniu do otoczenia zewnętrznego (możliwość prawnego egzekwowania przedmiotowych reguł).

¹⁰ *Op. cit.* 6.

2.3.1. Wiążący charakter reguł korporacyjnych dla przetwarzających w ramach organizacji¹¹

W tej kwestii można rozróżnić problem związany z zachowaniem zgodności z regułami oraz problem związany z możliwością ich prawnego egzekwowania.

Ocena „wiążącego charakteru” takich reguł korporacyjnych dla przetwarzających zakłada przeprowadzenie zwykłej oceny ich zewnętrznego i wewnętrznego charakteru wiążącego pod względem prawnym.

Wewnętrznie wiążący charakter tych reguł pod tym względem powodowałby obowiązek przestrzegania zasad wewnętrznych przez członków organizacji przetwarzającego oraz przez każdego jej pracownika. W związku z tym odpowiednie elementy mogłyby obejmować istnienie sankcji dyscyplinarnych nakładanych w przypadku naruszenia reguł, indywidualne i skuteczne informowanie pracowników, ustanowienie specjalnych programów kształcenia dla pracowników i podwykonawców itd. Wszystkie te elementy, które uwzględniono również w sekcji 4, mogłyby sprawić, że poszczególne osoby w organizacji przetwarzającego będą poczuwały się do przestrzegania wspomnianych reguł.

Jeżeli chodzi o członków grupy przetwarzającego, w gestii Grupy Roboczej Art. 29 nie leży określenie sposobu zagwarantowania przez organizację skutecznego zobowiązania wszystkich członków do przestrzegania przedmiotowych reguł lub ich poczucia obowiązku w odniesieniu do przestrzegania tych reguł, chociaż istnieją pewne znane przykłady w tym zakresie, takie jak wewnętrzne kodeksy postępowania poparte porozumieniami wewnątrzgrupowymi¹². Organizacje muszą jednak pamiętać, że podmioty ubiegające się o zatwierdzenie swoich wiążących reguł korporacyjnych dla przetwarzających dane jako odpowiednich zabezpieczeń zapewnionych przez przetwarzającego na rzecz administratora danych (art. 26 ust. 2 dyrektywy 95/46/UE) będą musiały wykazać wobec organów ochrony danych, że takie wiążące reguły korporacyjne dla przetwarzających są skutecznie wiążące dla całej grupy.

Wewnętrznie wiążący charakter reguł musi być wyraźny i na tyle odpowiedni, aby mógł zagwarantować zgodność z regułami poza UE, za co odpowiada zwykle siedziba główna w UE, członek z siedzibą w UE, któremu przekazano odpowiedzialność za ochronę danych lub przetwarzający eksporter danych w UE, który musi podjąć wszelkie niezbędne kroki, aby zagwarantować dostosowanie przez każdego członka jego działalności związanej z podprzetwarzaniem do zobowiązań określonych w wiążących regułach korporacyjnych¹³.

W większości przypadków faktycznie istnieje członek organizacji z siedzibą w UE, który zapewnia wystarczające zabezpieczenia i zajmuje się wnioskiem w sprawie wiążących reguł korporacyjnych dla przetwarzających składanym do głównego organu ochrony danych. Jeżeli siedziba organizacji jest zlokalizowana poza UE, siedziba powinna przekazać takie obowiązki członkowi, którego siedziba znajduje się w UE, o ile taki członek istnieje. Jest rzeczą

¹¹ Przyjęcie kodeksu postępowania jest krokiem, na który przedsiębiorstwa decydują się z trudem, ponieważ jego przyjęcie stwarza istotne ryzyko, a nawet powoduje konsekwencje prawne dla organizacji, które nie przestrzegają swojego własnego kodeksu.

¹² Należy zauważyć, że w niektórych państwach członkowskich jedynie umowy traktowane są jako wiążące. W związku z tym w przypadku zamiaru sięgnięcia po środki prawne inne niż umowy należałoby zasięgnąć porady na poziomie lokalnym.

¹³ W międzynarodowych podmiotach zależnych funkcjonujących na podstawie przepisów międzynarodowego prawa spółek istnieje możliwość wzajemnego egzekwowania kodeksów postępowania w drodze wniesienia roszczeń z tytułu naruszenia warunków umów dorozumianych, wprowadzenia w błąd i niedbalstwa.

oczywistą, że podmiot faktycznie zapewniający zabezpieczenia pozostaje odpowiedzialny za skuteczne zapewnianie zgodności z regułami oraz gwarantuje ich egzekwowanie. Można jednak dopuścić także inny mechanizm, tj. obciążenie odpowiedzialnością przetwarzającego eksportera danych w UE. Więcej informacji na ten temat przedstawiono w sekcjach 4.6 i 4.7 dotyczących odpowiedzialności i jurysdykcji.

2.3.2. Wiążący charakter reguł korporacyjnych dla przetwarzających w odniesieniu do zewnętrznych podmiotów podprzetwarzających dane

Jeżeli przetwarzający zleca podwykonawstwo swoich obowiązków na podstawie umowy o gwarantowanym poziomie usług (art. 17 dyrektywy) zewnętrznemu podmiotowi podprzetwarzającemu za zgodą administratora danych, odbywa się to wyłącznie w drodze pisemnej umowy z podprzetwarzającym. Więcej informacji na ten temat przedstawiono w sekcji 2.2.2. dotyczącej dalszego przekazywania danych.

2.3.3. Możliwość prawnego egzekwowania reguł korporacyjnych

2.3.3.1. Możliwość prawnego egzekwowania reguł korporacyjnych przez osoby, których dane dotyczą (prawa beneficjenta będącego osobą trzecią)

Osoby, których dane dotyczą, objęte zakresem wiążących reguł korporacyjnych dla przetwarzających muszą stać się beneficjentami będącymi osobami trzecimi poprzez włączenie klauzuli dotyczącej beneficjentów będących osobami trzecimi do wiążących reguł korporacyjnych, którym należy nadać moc wiążącą poprzez jednostronne zobowiązania (o ile pozwala na to prawo krajowe) lub poprzez ustalenia umowne między członkami grupy przetwarzającego.

W każdym przypadku osoby, których dane dotyczą, są uprawnione do egzekwowania zgodności z regułami wobec administratora danych, poprzez wniesienie skargi do organu ochrony danych lub do sądu właściwego dla administratora danych UE, zgodnie z wyjaśnieniem przedstawionym w sekcji 4.6.

W przypadku gdy osoby, których dane dotyczą, nie mogą wnieść skargi przeciwko administratorowi danych¹⁴, mogą one jednak wszcząć sprawę przeciwko przetwarzającemu także przed organem ochrony danych lub sądem właściwym dla (i) siedziby głównej przetwarzającego w UE, (ii) członka grupy podmiotu przetwarzającego w UE, któremu przekazano obowiązki dotyczące ochrony danych, lub (iii) przetwarzającego eksportera danych w UE.

Jeżeli jest to niemożliwe (na przykład w UE nie ma żadnego przedsiębiorstwa przetwarzającego), osoby, których dane dotyczą, są uprawnione do wniesienia skargi do sądu właściwego dla swojego miejsca zamieszkania. W każdym przypadku, jeżeli zgodnie z obowiązującym prawem krajowym istnieją bardziej korzystne rozwiązania w odniesieniu do osób, których dane dotyczą (jak w przypadku prawa konsumenckiego lub prawa pracy), wspomniane rozwiązania mają zastosowanie w takich okolicznościach.

¹⁴ Taka sytuacja może mieć miejsce, jeżeli administrator danych przestał istnieć faktycznie lub formalnie albo stał się niewypłacalny, o ile podmiot będący jego następcą nie przejął wszystkich zobowiązań prawnych administratora danych na podstawie umowy lub z mocy prawa, a wówczas osoby, których dane dotyczą, mogą egzekwować przysługujące im prawa wobec takiego podmiotu.

Podczas gdy w niektórych przypadkach możliwość prawnego egzekwowania klauzuli dotyczącej beneficjenta będącego osobą trzecią, zawartej w jednostronnych oświadczeniach, nie budzi żadnych wątpliwości, w innych państwach członkowskich sytuacja nie jest aż tak oczywista, a jednostronne oświadczenia mogą okazać się niewystarczające. W przypadku gdy nie można uznać, że jednostronne oświadczenia przyznają możliwe do wyegzekwowania prawa beneficjenta będącego osobą trzecią, organizacje będą musiały wprowadzić niezbędne ustalenia umowne umożliwiające przyznanie takich praw. Ustalenia umowne mogą być prawnie egzekwowane na mocy prawa prywatnego we wszystkich państwach członkowskich¹⁵.

Zasady określone w wiążących regułach korporacyjnych, które mają stać się możliwe do wyegzekwowania na mocy klauzuli dotyczącej praw beneficjenta będącego osobą trzecią, są następujące:

- obowiązek przetwarzającego dotyczący przestrzegania wiążących reguł korporacyjnych oraz instrukcji administratora danych w zakresie przetwarzania danych, jak również środków ochrony i poufności przewidzianych w umowie o gwarantowanym poziomie usług (WP195 sekcja 1.1);
- ustanowienie praw beneficjenta będącego osobą trzecią w odniesieniu do osób, których dane dotyczą (WP195, sekcja 1.3);
- odpowiedzialność przetwarzającego za zapłatę odszkodowania oraz podjęcia działań naprawczych w przypadkach naruszenia wiążących reguł korporacyjnych (WP195 sekcja 1.5);
- ciężar dowodu spoczywający na przetwarzającym, a nie na osobach, których dane dotyczą (WP195 sekcja 1.7);
- łatwy dostęp do wiążących reguł korporacyjnych dla osób, których dane dotyczą (WP195, sekcja 1.8);
- istnienie procedury rozpatrywania skarg w zakresie wiążących reguł korporacyjnych (WP195 sekcja 2.2);
- obowiązek prowadzenia współpracy z organami ochrony danych (WP195 sekcja 3.1) oraz z administratorem danych (WP195 sekcja 3.2);
- zasady prywatności (WP195 sekcja 6.1);
- lista podmiotów przetwarzających podlegających wiążącym regułom korporacyjnym (WP195 sekcja 6.2);
- przejrzystość w przypadkach, w których przepisy krajowe uniemożliwiają przetwarzającemu zachowanie zgodności z wiążącymi regułami korporacyjnymi (WP195 sekcja 6.3).

¹⁵ Obecnie istnieje możliwość przyznania w umowie praw beneficjenta będącego osobą trzecią we wszystkich państwach członkowskich. W tym względzie zob. poprzednie doświadczenia w zakresie standardowych klauzul umownych oraz beneficjentów będących osobą trzecią.

Ustalenia umowne nie muszą być złożone ani długie. Są one jedynie instrumentami służącymi do zastosowania praw beneficjenta będącego osobą trzecią na rzecz osób fizycznych w tych państwach, w których mogą zachodzić wątpliwości w odniesieniu do tego, czy jednostronne oświadczenia mają podobny skutek. W niektórych przypadkach jest to możliwe poprzez dodanie prostej klauzuli w innych umowach zawieranych między członkami grupy przetwarzającego.

2.3.3.2. Możliwość prawnego egzekwowania reguł korporacyjnych przez administratora danych

Wiążące reguły korporacyjne dla przetwarzających stanowią zabezpieczenie dla międzynarodowego przekazywania danych zapewniane przez przetwarzającego na rzecz jego klienta (administratora danych), przy czym to administrator danych jest w głównej mierze odpowiedzialny przed organami ochrony danych oraz osobami, których dane dotyczą, za zapewnienie ochrony danych osobowych przekazywanych poza UE. W związku z tym wiążące reguły korporacyjne dla przetwarzających wiążą administratora danych na mocy szczególnego odniesienia do tych reguł w umowie o gwarantowanym poziomie usług.

Dodatkowo w celu zapewnienia jednoznacznego powiązania wiążących reguł korporacyjnych dla przetwarzających z umową o gwarantowanym poziomie usług podpisywaną z każdym klientem (administratorem danych) należy upewnić się, że w umowie o świadczenie usług uregulowane są następujące kwestie:

- jeżeli przekazywanie danych obejmuje szczególną kategorię danych, administrator danych zobowiązuje się, że osoby, których dane dotyczą, zostały lub zostaną poinformowane przed przekazaniem danych o tym, że ich dane mogą zostać przekazane do państwa trzeciego niezapewniającego odpowiedniej ochrony;
- administrator danych zobowiązuje się także do poinformowania osób, których dane dotyczą, o istnieniu przetwarzających z siedzibą poza UE oraz wiążących reguł korporacyjnych dla przetwarzających. Administrator danych udostępnia osobom, których dane dotyczą, na ich wniosek kopię wiążących reguł korporacyjnych dla przetwarzających oraz umowy o gwarantowanym poziomie usług (z pominięciem wszelkich szczególnie chronionych i poufnych informacji handlowych).
- określone są przejrzyste środki poufności i środki ochrony lub są one przedmiotem odesłania z podaniem łącza elektronicznego;
- przedstawiono przejrzysty opis instrukcji oraz przetwarzania danych;
- w umowie o gwarantowanym poziomie usług precyzyjnie określono, czy dane mogą być podprzetwarzane w ramach grupy przetwarzającego lub poza tą grupą oraz czy uprzednia zgoda wydana przez administratora danych ma charakter ogólny, czy też należy ją wydawać w odniesieniu do każdego nowo podejmowanych działań związanych z podprzetwarzaniem.

Organy ochrony danych przeprowadzające ocenę wiążących reguł korporacyjnych mogą nie wymagać przedstawienia im takiej umowy o gwarantowanym poziomie usług, jednak we wszystkich przypadkach należy przedłożyć formularz ze streszczeniem oraz fragmentami zaczerpniętymi ze wspomnianej umowy w celu wyjaśnienia, w jaki sposób administratorzy egzekwują wiążące reguły korporacyjne dla przetwarzających.

Ponadto wiążące reguły korporacyjne będą zawierać klauzulę dotyczącą prawa beneficjenta będącego osobą trzecią na korzyść administratora danych, aby zapewnić jego uprawnienie do egzekwowania wiążących reguł korporacyjnych wobec każdego członka grupy podmiotu przetwarzającego, obejmujące zastosowanie sądowych środków odwoławczych oraz prawo do otrzymania odszkodowania.

2.3.3.3. Możliwość prawnego egzekwowania reguł korporacyjnych przez organy ochrony danych

Jeżeli przetwarzający składa wniosek o uznanie przez UE jego wiążących reguł korporacyjnych dla przetwarzających za odpowiednie zabezpieczenie zapewniane przez przetwarzającego na rzecz administratora danych (art. 26 ust. 2 dyrektywy 95/46/UE), jasne jest, że grupa przetwarzającego zobowiązuje się wobec organów ochrony danych UE do przestrzegania zapewnionych zabezpieczeń (w tym przypadku wiążących reguł korporacyjnych dla przetwarzających). Niemniej jednak to administrator danych będzie odpowiedzialny za ubieganie się o wydanie wymaganego krajowego zezwolenia na międzynarodowe przekazywanie danych, które należy wyraźnie odróżnić od uznawania wiążących reguł korporacyjnych za zapewniające wystarczające zabezpieczenia dla przekazywania danych. Administrator będzie się odnosił do wiążących reguł korporacyjnych dla przetwarzających, które już „zatwierdzono” (nie do tych, dla których „wydano zezwolenie”) na szczelbu UE jako do właściwych zabezpieczeń proponowanych w odniesieniu do międzynarodowego przekazywania danych.

Art. 28 dyrektywy 95/46/UE stanowi, że organy ochrony danych są „odpowiedzialne za kontrolę stosowania na ich terytorium przepisów przyjętych przez Państwa Członkowskie na mocy niniejszej dyrektywy”, co oznacza, że organy te mają m.in. obowiązek sprawowania nadzoru nad przekazywaniem danych oraz przeprowadzania ocen gwarancji w zakresie przekazywania danych poza UE.

Aby realizować taki zakres obowiązków, organy ochrony danych są wyposażone w uprawnienia do prowadzenia dochodzeń, skuteczne uprawnienia interwencyjne na swoim terytorium, jak również uprawnienie do wszczynania postępowań prawnych; uprawnienia takie mogą być stosowane przeciwko przetwarzającemu, który nie przestrzegał wiążących reguł korporacyjnych.

Ponadto naruszenie wiążących reguł korporacyjnych dla przetwarzających przez członka grupy podmiotu przetwarzającego (lub przez całą grupę) może prowadzić do wycofania zezwolenia na odnośne przekazywanie danych udzielonego administratorowi danych na podstawie wiążących reguł korporacyjnych dla przetwarzających. Takie wycofanie nie ma mocy wstecznej.

2.3.4. Obowiązkowe wymagania ustawodawstwa krajowego mające zastosowanie do członków organizacji

Wiążące reguły korporacyjne powinny zawierać przejrzyste postanowienie, że w przypadkach, w których członek grupy przetwarzającego ma powody, żeby sądzić, iż istniejące lub przyszłe przepisy mające do niego zastosowanie mogą uniemożliwiać mu wykonywanie instrukcji otrzymywanych od administratora danych lub jego obowiązków wynikających z wiążących reguł korporacyjnych lub umowy o gwarantowanym poziomie usług, powiadomi on niezwłocznie o tym fakcie następujące podmioty:

- administratora danych, który jest uprawniony do zawieszenia przekazywania danych lub wypowiedzenia umowy o gwarantowanym poziomie usług oraz
- siedzibę główną przetwarzającego w UE lub członka z siedzibą w UE, któremu przyznano obowiązki w zakresie ochrony danych lub odpowiedniego urzędnika/pracownika ds. prywatności u przetwarzającego oraz
- organ ochrony danych właściwy dla administratora danych.

Ponadto przetwarzający informuje administratora danych o jakichkolwiek prawnie wiążących wnioskach o ujawnienie danych osobowych ze strony organów ścigania, chyba że powiadomienie o takim wniosku jest zabronione, na przykład na mocy prawa karnego w celu zachowania poufności postępowań prowadzonych przez organy ścigania. W każdym przypadku należy wstrzymać wniosek o ujawnienie oraz wyraźnie poinformować o tym fakcie organy ochrony danych właściwe dla administratora danych i główny organ ochrony danych ds. wiążących reguł korporacyjnych dla przetwarzających.

Niezbędne będzie jednak również zapewnienie przekazywania danych osobowych do organów ścigania w oparciu o podstawy prawne określone w obowiązujących przepisach, o ile wymogi w zakresie wiążących reguł korporacyjnych dla przetwarzających przedstawione zawarte w sekcji 6.3 WP195 przewidują wyłącznie taki proces przekazywania informacji (zob. powyżej), który nie uprawnia do przekazywania danych. W przypadku spraw powiązanych z prawem różnych państw należy odnosić się do traktatów i porozumień międzynarodowych, mających zastosowanie do takich spraw.

3. ZAWARTOŚĆ MERYTORYCZNA WIĄŻĄCYCH REGUŁ KORPORACYJNYCH DLA PRZETWARZAJĄCYCH

3.1. Zawartość merytoryczna i poziom szczegółowości

Zasady ochrony danych określone w dyrektywie należy rozwinąć i uszczegółowić w wiążących regułach korporacyjnych dla przetwarzających, tak aby były dostosowane w sposób praktyczny i realistyczny do działalności związanej z przetwarzaniem prowadzonej przez organizację w państwach trzecich oraz mogły być zrozumiane i skutecznie stosowane przez podmioty pełniące obowiązki związane z ochroną danych w ramach organizacji.

W sekcji 6 WP195 zawarto szersze wyjaśnienie tej zawartości.

W wiążących regułach korporacyjnych można zawrzeć jedynie ogólny opis przekazywanych danych, jednak w ramach krajowej procedury wydawania zezwoleń konieczne będzie przedstawienie organom ochrony danych bardziej precyzyjnych informacji na temat poszczególnych przypadków przekazywania danych przez określonego administratora danych. Poziom szczegółowości wiążących reguł korporacyjnych musi być wystarczająca, aby umożliwić organom ochrony danych dokonanie oceny, czy zostały zapewnione właściwe zabezpieczenia w zakresie przetwarzania oraz podprzetwarzania danych prowadzonego w państwach trzecich przez członka grupy podmiotu przetwarzającego.

3.2. Aktualizacja wiążących reguł korporacyjnych

Grupa Robocza Art. 29 uznaje, że organizacje są podmiotami ewoluującymi, których członkowie i praktyki mogą podlegać regularnym zmianom, tak aby dane przekazywane w imieniu i zgodnie z instrukcjami administratorów danych oraz, siłą rzeczy, zasady zawarte w wiążących regułach korporacyjnych nie mogły nieustannie odpowiadać rzeczywistości, która istniała w czasie uznania zabezpieczenia za odpowiednie.

W związku z tym wiążące reguły korporacyjne dla przetwarzających można modyfikować (na przykład w celu uwzględnienia zmian w otoczeniu regulacyjnym lub strukturze organizacyjnej), muszą one jednak nakładać obowiązek informowania o zmianach wszystkich członków grupy, organów ochrony danych oraz administratora danych.

Jeżeli zmiana wpływa na warunki przetwarzania, informacje należy przekazywać administratorowi danych z takim wyprzedzeniem czasowym, które umożliwi administratorowi danych zakwestionowanie danej zmiany lub wypowiedzenie umowy przed wprowadzeniem modyfikacji (na przykład w zakresie wszelkich zamierzonych zmian w zakresie wyboru dodatkowych podwykonawców lub ich zastąpienia, zanim dane zostaną przekazane nowemu podprzetwarzającemu).

Aktualizacje wiążących reguł korporacyjnych dla przetwarzających lub wykazu członków wiążących reguł korporacyjnych dla przetwarzających są możliwe bez konieczności ponownego składania wniosku do organów ochrony danych, o ile spełnione są następujące warunki:

- i) wyznaczona osoba prowadzi w pełni zaktualizowany wykaz członków grupy oraz podprzetwarzających biorących udział w działalności związanej z przetwarzaniem danych na rzecz administratora danych, przy czym wykaz ten jest udostępniany administratorowi danych, osobom, których dane dotyczą oraz organom ochrony danych;
- ii) wspomniana osoba będzie monitorować i rejestrować wszelkie aktualizacje reguł oraz będzie regularnie dostarczać niezbędne informacje administratorowi danych oraz na wniosek organów ochrony danych;
- iii) nowemu członkowi nie przekazuje się żadnych danych, dopóki nie będzie od w sposób skuteczny podlegał wiążącym regułom korporacyjnym dla przetwarzających i nie zapewni zgodności;
- iv) informacje o wszelkich istotnych zmianach w wiążących regułach korporacyjnych dla przetwarzających lub w wykazie członków są przekazywane raz w roku organom ochrony danych wydającym zezwolenia na przekazywanie danych administratorowi (administratorom) danych, wraz z krótkim wyjaśnieniem powodów uzasadniających daną aktualizację.

Przez aktualizację reguł należy rozumieć fakt, iż procedury pracy mogą ulegać zmianom, a reguły muszą być dostosowywane do tego typu przypadków zmieniającego się otoczenia.

4. ZAPEWNIENIE ZGODNOŚCI I GWARANCJA EGZEKWOWANIA

Poza wspomnianymi regułami dotyczącymi istotnych zasad ochrony danych wszelkie wiążące reguły korporacyjne dla przetwarzających muszą także zawierać poniższe elementy.

4.1. Przepisy gwarantujące istotny poziom zgodności

Oczekuje się, że dzięki przedmiotowym regułom ustanowiony zostanie system gwarantujący świadomość ich istnienia oraz ich wdrożenie zarówno w Unii Europejskiej, jak i poza nią. Określanie przez siedzibę główną wewnętrznych polityk ochrony prywatności należy traktować jedynie jako pierwszy krok w procesie zapewniania wystarczających zabezpieczeń w rozumieniu art. 26 ust. 2 dyrektywy. Organizacja wnioskująca musi być także w stanie wykazać, że taka polityka jest znana, zrozumiała i skutecznie stosowana w grupie przez pracowników, którzy przeszli odpowiednie szkolenie i dysponują istotnymi informacjami (w tym wiążącymi regułami korporacyjnymi), które są nieustannie dostępne, np. za pośrednictwem internetu. Organizacja powinna wyznaczyć odpowiedni personel, przy wsparciu osób zarządzających wyższego szczebla, którego zadaniem będzie sprawowanie nadzoru i zapewnianie zgodności.

4.2. Audyty

Reguły muszą przewidywać przeprowadzanie regularnych audytów w zakresie ochrony danych lub sprawowanie regularnego zewnętrznego nadzoru przez wewnętrznych lub zewnętrznych akredytowanych audytorów, odpowiadających bezpośrednio przed urzędnikiem/pracownikiem ds. ochrony prywatności oraz zarządem spółki dominującej najwyższego szczebla i pozostających do dyspozycji na wezwanie administratora danych¹⁶.

Wiążące reguły korporacyjne dla przetwarzających muszą również stanowić, że organy ochrony danych właściwe dla administratora danych mogą uzyskać dostęp do wyników wspomnianych audytów na wniosek oraz uzyskiwać uprawnienia do samodzielnego przeprowadzania audytów w zakresie ochrony danych, o ile jest to konieczne i możliwe z punktu widzenia prawa. Dzieje się tak najczęściej w przypadku, gdy audyty, o których mowa w poprzednim akapicie, nie były dostępne z dowolnych powodów, nie zawierały istotnych informacji niezbędnych do podjęcia typowych działań następczych w związku z wydaniem zezwolenia przez organy ochrony danych lub w wyniku niecierpiącej zwłoki sytuacji preferowany byłby bezpośredni udział organu ochrony danych właściwego dla administratora danych.

Takie audyty odbywałyby się zgodnie z odpowiednimi przepisami i uregulowaniami ustanawiającymi uprawnienia do prowadzenia dochodzeń organów ochrony danych, nie powodując uszczerbku dla uprawnień kontrolnych każdego z organów ochrony danych. Tak czy inaczej audyty będą przeprowadzane z zachowaniem pełnego poszanowania dla poufności i tajemnic handlowych i ograniczałyby się wyłącznie do ustalenia zgodności z wiążącymi regułami korporacyjnymi.

Ponadto wiążące reguły korporacyjne dla przetwarzających stanowią, że każdy przetwarzający lub podprzetwarzający zajmujący się danymi określonego administratora danych wyrazi zgodę, na wniosek danego administratora danych, na przeprowadzenie audytu w jego obiektach przetwarzania danych w odniesieniu do prowadzonej przez danego administratora danych działalności związanej z przetwarzaniem. Taki audyt powinien być przeprowadzany przez administratora danych lub organ kontrolny złożony z niezależnych

¹⁶ Wspomniane audyty muszą być merytorycznie kompleksowe i złożone pod względem każdej kwestii dotyczącej szczegółów wskazanych już w niniejszym dokumencie roboczym, takich jak istnienie dalszego przekazywania danych na podstawie standardowych klauzul umownych (zob. sekcja 2.2.2.) lub decyzje podejmowane w odniesieniu do obowiązkowych wymogów zgodnie z prawem krajowym, które może wchodzić w konflikt z wiążącymi regułami korporacyjnymi (zob. sekcja 3.3.3.).

członków posiadających wymagane kwalifikacje zawodowe, związanych obowiązkiem zachowania poufności, wybranych przez administratora danych, w stosownych przypadkach, w porozumieniu z właściwym dla niego organem ochrony danych.

Formularz zgłoszeniowy zawiera opis systemu audytowego. Opis ten przedstawia przykładowo następujące informacje:

- który podmiot (wydział w grupie) decyduje o planie/programie audytu;
- który podmiot będzie przeprowadzał audyt;
- Termin przeprowadzania audytu (regularnie czy na szczególny wniosek odpowiedniego pracownika ds. ochrony prywatności);
- zakres audytu (np. aplikacje, systemy IT, bazy danych przetwarzające dane osobowe, dalsze przekazywanie danych, decyzje podejmowane w odniesieniu do obowiązkowego wymogu regulowanego w prawie krajowym, który jest niezgodny z wiążącymi regułami korporacyjnymi dla przetwarzających, przegląd warunków umownych stosowanych w odniesieniu do przekazywania danych poza grupę przetwarzającego (do administratorów lub przetwarzających), działania naprawcze itd.);
- który podmiot otrzyma wyniki audytów.

4.3. Rozpatrywanie skarg

Wiążące reguły korporacyjne dla przetwarzających zawierają zobowiązanie grupy przetwarzającego do ustanowienia specjalnego punktu kontaktowego dla osób, których dane dotyczą.

Wszyscy członkowie podlegający wiążącym regułom korporacyjnym dla przetwarzających są zobowiązani jedynie do niezwłocznego przekazania skargi lub wniosku administratorowi danych, bez obowiązku ich rozpatrywania (chyba, że ustalono inaczej z administratorem danych).

Jedynie w przypadku, gdy administrator danych przestał istnieć faktycznie lub formalnie albo stał się niewypłacalny, przekazywaniem wszelkich skarg i wniosków musi zająć się przetwarzający.

W przypadkach, w których skargi są rozpatrywane przez przetwarzającego (tj. gdy zostało to uzgodnione z administratorem danych lub administrator danych przestał istnieć faktycznie lub formalnie), zajmuje się nimi wydział lub osoba wyznaczeni konkretnie do tego celu, posiadający odpowiedni poziom niezależności w sprawowaniu swoich funkcji.

W takich przypadkach osobom, których dane dotyczą, podaje się następujące informacje:

- gdzie składać skargę;
- w jakiej formie;
- termin udzielenia odpowiedzi na skargę;
- konsekwencje w przypadku odrzucenia skargi;

- konsekwencje w przypadku uznania skargi za uzasadnioną;
- konsekwencje w przypadku, gdy osoba, której dane dotyczą, jest nieusatysfakcjonowana odpowiedzią (prawo do złożenia skargi do sądu/organów ochrony danych).

4.4. Obowiązek współpracy z administratorem danych

W wiążących regułach korporacyjnych dla przetwarzających wyraźnie stwierdzono, że wszyscy członkowie grupy oraz pracownicy powinni przestrzegać instrukcji administratora danych w zakresie przetwarzania danych oraz środków ochrony i poufności określonych w umowie o gwarantowanym poziomie usług (art. 17 dyrektywy).

W regułach określono także wyraźnie, że każdy przetwarzający lub podprzetwarzający ma obowiązek współpracować z administratorem danych i wspierać go, aby zapewnić zgodność z przepisami dotyczącymi ochrony danych (np. wywiązywać się z obowiązku przestrzegania praw osób, których dane dotyczą, lub rozpatrywania ich skarg, lub być w stanie reagować na dochodzenia lub zapytania ze strony organów ochrony danych). Odbywa się to w odpowiednim czasie i w możliwie najbardziej odpowiednim zakresie.

4.5. Obowiązek współpracy z organami ochrony danych

Jak przedstawiono w WP 12, jednym z najważniejszych elementów oceny adekwatności systemu samoregulacyjnego jest poziom wsparcia i pomocy dostępnych dla poszczególnych osób, których dane dotyczą: „Głównym wymogiem właściwego i skutecznego systemu ochrony danych jest dopilnowanie, aby osoba, która napotyka problemem dotyczący jej danych osobowych, nie została pozostawiona sama sobie, lecz otrzymała określone wsparcie instytucjonalne, pozwalające na rozwiązanie napotkanych przez nią trudności”.

Jest to istotny element wiążących reguł korporacyjnych dla przetwarzających: w regułach należy wyraźnie określić zobowiązanie wszystkich członków grupy przetwarzającego do współpracy z organami ochrony danych właściwymi dla odpowiedniego administratora danych, tak aby poszczególne osoby mogły korzystać ze wsparcia instytucjonalnego, o którym mowa w dokumencie roboczym 12.

Ponadto należy jednoznacznie określić zobowiązanie, w myśl którego organizacja jako całość oraz każdy z jej członków z osobna będą przestrzegać porad udzielanych przez właściwe organy ochrony danych we wszelkich kwestiach związanych z interpretacją i stosowaniem wspomnianych wiążących reguł korporacyjnych dla przetwarzających.

Przed udzieleniem jakichkolwiek porad właściwe organy ochrony danych mogą zabiegać o uzyskanie opinii organizacji, zainteresowanych osób, których dane dotyczą, odpowiedniego administratora danych oraz organów ochrony danych, które mogą być zaangażowane ze względu na skoordynowaną procedurę przewidzianą w niniejszym dokumencie roboczym¹⁷. Porada udzielona przez organ może zostać upubliczniona.

Oprócz sankcji przewidzianych w jakimkolwiek odnośnym przepisie na szczeblu krajowym zasadnicze lub uporczywe odmawianie przez organizację podjęcia współpracy lub zastosowania się do porady właściwego organu ochrony danych może skutkować zawieszeniem lub cofnięciem zezwolenia na przekazywanie danych udzielonego odpowiedniemu administratorowi danych (odpowiednim administratorom danych), którego

¹⁷ Zob. rozdział 5.

dokonyuje sam organ ochrony danych lub właściwy organ upoważniony do tych czynności na mocy prawa krajowego. Bezpośrednią konsekwencją takiego zawieszenia lub cofnięcia będzie konieczność znalezienia przez odpowiedniego administratora danych innego sposobu zapewnienia właściwej ochrony przekazywanych danych, na przykład poprzez podpisanie standardowych klauzul umownych 2010/87/UE oraz złożenie ponownego wniosku w sprawie przekazywania tych danych do właściwych organów ochrony danych zgodnie z obowiązującym ustawodawstwem krajowym.

4.6. Odpowiedzialność

4.6.1. Ogólne prawo do otrzymania zadośćuczynienia oraz stosownego odszkodowania

W regułach należy wskazać, że prawa beneficjenta będącego osobą trzecią przyznane osobie, której dane dotyczą, oraz prawo do otrzymania zadośćuczynienia przyznane administratorowi danych powinny obejmować sądowe środki odwoławcze oraz prawo do otrzymania odszkodowania z tytułu każdej szkody (w przypadku osoby, której dane dotyczą, powinna ona obejmować zarówno szkodę materialną, jak również każde cierpienie psychiczne).

W uzupełnieniu tego ogólnego prawa reguły muszą zawierać także postanowienia dotyczące odpowiedzialności i jurysdykcji, których celem jest ułatwienie jego wykonania w praktyce.

4.6.2. Reguły dotyczące odpowiedzialności

4.6.2.1. Reguły dotyczące odpowiedzialności dla osób, których dane dotyczą

Osoby, których dane dotyczą, jako beneficjenci będący osobami trzecimi są uprawnione do egzekwowania wiążących reguł korporacyjnych w odniesieniu do członków grupy przetwarzającego, którzy takie reguły naruszyli.

Ponadto w wiążących regułach korporacyjnych dla przetwarzających wskazuje się członka grupy spośród następujących jednostek: (i) siedziby głównej w UE; lub (ii) członka podmiotu przetwarzającego z siedzibą w UE, któremu przekazano obowiązki ochrony danych; lub (iii) przetwarzającego eksportera w UE (np. mająca siedzibę w UE strona umawiająca się z administratorem danych), który odpowiada za podjęcie odpowiednich kroków i zgadza się na ich podjęcie w celu naprawienia działań innych członków organizacji mającej siedzibę poza UE (w przypadku naruszenia przez nich wiążących reguł korporacyjnych lub umowy o świadczenie usług) lub naruszeń umowy pisemnej (o której mowa w sekcji 2.2.2.), których dopuścili się zewnętrznym podprzetwarzającym mającym siedzibę poza UE oraz, w stosownych przypadkach, do zapłacenia odszkodowania za wszelkie powstałe szkody. Jeżeli organizacja wybiera trzeci wariant (przetwarzający eksporter w UE), organizacja przedstawia głównemu organowi ochrony danych wyjaśnienie przyczyn, które uniemożliwiają, by funkcjonował podmiot odpowiedzialny za całą grupę.

W miejsce członka grupy spoza UE lub zewnętrznego podprzetwarzającego mającego siedzibę poza UE, który naruszył wiążące reguły korporacyjne, odpowiedzialność bierze na siebie wyznaczony członek przedsiębiorstwa, tak jakby to on sam dopuścił się naruszenia w państwie członkowskim, w którym ma swoją siedzibę.

Członek ten nie może liczyć na to, że uniknie ciążącej na nim odpowiedzialności powołując się na niedopełnienie obowiązków przez podprzetwarzającego (wewnętrznego lub zewnętrznego podprzetwarzającego grupy).

W przypadku gdy żaden z członków organizacji nie ma swojej siedziby w UE, odpowiedzialność tę bierze na siebie siedziba główna grupy zlokalizowana poza UE.

4.6.2.2. Reguły dotyczące odpowiedzialności w odniesieniu do administratora danych

Wiążące reguły korporacyjne dla przetwarzających muszą przewidywać uprawnienie wszystkich administratorów danych do egzekwowania tych reguł wobec każdego członka grupy podmiotu przetwarzającego z powodu naruszeń, których się on dopuścił. Administrator danych powinien być także uprawniony do egzekwowania pisemnej umowy (o której mowa w sekcji 2.2.2.) wobec wszelkich zewnętrznych podprzetwarzających będących źródłem naruszeń.

Ponadto, w przypadku gdy naruszenia dopuściła się jednostka przetwarzającego spoza UE lub zewnętrzny podprzetwarzający spoza UE, administrator danych ma prawo egzekwować wiążące reguły korporacyjne dla przetwarzających wobec podmiotu przetwarzającego, który wziął na siebie odpowiedzialność¹⁸ oraz podjąć działania naprawcze w związku z naruszeniami wiążących reguł korporacyjnych, umowy o świadczenie usług lub pisemnych umów zawartych z zewnętrznymi podprzetwarzającymi.

Organizacja zobowiąże się w swoim formularzu zgłoszeniowym dotyczącym wiążących reguł korporacyjnych dla przetwarzającego do tego, aby podmiot, który wziął na siebie odpowiedzialność za działania innych członków podlegających wiążącym regułom korporacyjnym dla przetwarzających spoza UE oraz zewnętrznych podprzetwarzających z siedzibą poza UE, dysponował aktywami wystarczającymi do wypłacenia odszkodowania za zaistniałe szkody.

4.6.2.3. Reguły dotyczące ciężaru dowodu

Wiążące reguły korporacyjne dla przetwarzających muszą także określać, że jeżeli osoby, których dane dotyczą, lub administratora danych, mogą wykazać, że ponieśli szkody oraz ustalić fakty wskazujące na istnienie prawdopodobieństwa, że szkoda powstała w wyniku naruszenia wiążących reguł korporacyjnych dla przetwarzających (lub umowy o świadczenie usługi czy też pisemnych umów, o których mowa w sekcji 2.2.2), członek grupy, który wziął na siebie odpowiedzialność, jest zobowiązany udowodnić, że członek organizacji spoza UE ani zewnętrzny podprzetwarzający nie byli odpowiedzialni za naruszenie, które doprowadziło do wspomnianych szkód, lub że żadne takie naruszenie nie miało miejsca.

Jeżeli podmiot, który wziął na siebie odpowiedzialność, udowodni, że członek grupy spoza UE nie jest odpowiedzialny za dane działanie, może on zostać zwolniony z ponoszenia jakiegokolwiek odpowiedzialności.

¹⁸ Siedziba główna przetwarzającego w UE lub członek podmiotu przetwarzającego z siedzibą w UE, któremu przekazano obowiązki związane z ochroną danych lub przetwarzający eksporter danych w UE (zob. WP195 sekcja 1.5).

4.7. Reguła dotycząca jurysdykcji

Jak wyjaśniono powyżej, w rozdziale 4.6.2., organizacja musi również zgodzić się na to, aby osoby, których dane dotyczą, były uprawnione do wszczęcia postępowania przeciwko organizacji w przypadku, gdy nie są w stanie wnieść powództwa przeciwko administratorowi danych¹⁹, jak również do wyboru jurysdykcji (organu ochrony danych lub sądu):

- a) właściwych organów ochrony danych; lub
- b) jurysdykcji członka podmiotu przetwarzającego w UE, który jest źródłem przekazanych danych; lub
- c) jurysdykcji europejskiej siedziby głównej przetwarzającego; lub
- d) jurysdykcji europejskiego członka podmiotu przetwarzającego, któremu przekazano odpowiedzialność za ochronę danych; lub
- e) w przypadku, gdy żaden z członków organizacji nie ma swojej siedziby w UE, osoby, których dane dotyczą oraz administrator danych są uprawnieni do wniesienia skargi do organów ochrony danych lub sądów właściwych dla ich miejsca zamieszkania/siedziby. Jeżeli osoba, której dane dotyczą, lub administrator danych ma miejsce zamieszkania/ siedzibę poza UE i wnosi skargę do sądu spoza UE, właściwe organy ochrony danych UE powinny zostać poinformowane o istnieniu takiego powództwa i jego wyniku.

Przy właściwym funkcjonowaniu systemu, który zakłada dobry poziom zgodności w grupie, regularnych audytach, efektywnym rozpatrywaniu skarg, współpracy z organami ochrony danych itd., udział sądów wydaje się mało prawdopodobny, nie można go jednak w żadnym wypadku wykluczyć. Tym samym jedynie doświadczenie w zakresie tych instrumentów wykaże, czy taka prognoza jest prawidłowa.

Odpowiednie zasady i reguły dotyczące jurysdykcji, zawarte zarówno w dyrektywie, jak i w przepisach krajowych, pozostaną w mocy.

4.8. Przejrzystość

Organizacje, które wdrażają wiążące reguły korporacyjne dla przetwarzających, muszą mieć możliwość wykazania, że osoby, których dane dotyczą, mają łatwy dostęp do korzystania ze wszystkich zobowiązań podjętych zgodnie z tymi regułami, które mają prawo egzekwować jako beneficjenci będący osobami trzecimi. W związku z tym na stronach internetowych organizacji publikuje się w sposób łatwo dostępny dla osób, których dane dotyczą, wiążące reguły korporacyjne dla przetwarzających lub przynajmniej dokument zawierający wszystkie informacje (a nie ich streszczenie) dotyczące praw beneficjentów będących osobami trzecimi określonych w rozdziale 2.3.3.1.

¹⁹ Taka sytuacja może mieć miejsce, jeżeli administrator danych przestał istnieć faktycznie lub formalnie albo stał się niewypłacalny, o ile podmiot będący jego następcą nie przejął wszystkich zobowiązań prawnych administratora danych na podstawie umowy lub z mocy prawa, a wówczas osoby, których dane dotyczą, mogą egzekwować przysługujące im prawa wobec takiego podmiotu.

Jeżeli chodzi o administratora danych, umowa o świadczenie usług zapewnia włączenie wiążących reguł korporacyjnych dla przetwarzających do umowy. Wiążące reguły korporacyjne dla przetwarzających zostaną załączone do umowy o świadczenie usług lub możliwe będzie odesłanie do nich za pomocą dostępu elektronicznego.

5. WNIOSEK

Grupa Robocza Art. 29 uważa, że wytyczne określone w niniejszym dokumencie mogą ułatwić stosowanie art. 26 ust. 2 dyrektywy w przypadku wiążących reguł korporacyjnych dla przetwarzających. W pewnym stopniu powinny one także skutkować uproszczeniem dla wielonarodowych organizacji zajmujących się nieustannie przetwarzaniem i wymianą danych osobowych na szczeblu światowym w imieniu administratorów danych.

Nie należy traktować treści niniejszego dokumentu roboczego jako ostatecznego poglądu Grupy Roboczej Art. 29 w tej kwestii, lecz raczej jako pierwszy, zdecydowany krok mający na celu podkreślenie możliwości stosowania wiążących reguł korporacyjnych dla przetwarzających na podstawie podejścia samoregulacyjnego oraz współpracy między organami, bez uszczerbku dla możliwości stosowania innych narzędzi w odniesieniu do przekazywania danych osobowych za granicę, takich jak, w stosownych przypadkach, standardowe klauzule umowne lub zasady bezpiecznego transferu danych osobowych.

Mile widziany będzie dalszy wkład ze strony zainteresowanych kręgów i ekspertów wnoszony na podstawie ich doświadczeń zdobywanych w trakcie stosowania niniejszego dokumentu. Grupa Robocza Art. 29 może podjąć decyzję o ponownym zajęciu się przedmiotowym zagadnieniem w oparciu o zdobyte doświadczenia.

Sporządzono w Brukseli dnia 19 kwietnia 2013 r.

W imieniu grupy roboczej

Przewodniczący

Jacob Kohnstamm