GRUPA ROBOCZA ARTYKUŁU 29 DS. OCHRONY DANYCH

WP 153

Dokument roboczy ustanawiający tabelę zawierającą elementy i zasady, które mają być uwzględnione w Wiążących Regułach Korporacyjnych

Przyjęty 24 czerwca 2008 r.

Niniejsza Grupa Robocza została powołana na mocy artykułu 29 Dyrektywy 95/46/WE. Jest to niezależny europejski organ doradczy w sprawach ochrony danych i prywatności. Jego zadania opisane zostały w artykule 30 Dyrektywy 95/46/WE i artykule 15 Dyrektywy 2002/58/WE.

Obsługę Sekretariatu zapewnia Dyrekcja C (Sądownictwo Cywilne, Prawa i Obywatelstwo) Komisji Europejskiej, Dyrekcja Generalna ds. Sprawiedliwości, Wolności i Bezpieczeństwa, B-1049 Bruksela, Belgia, Biuro nr LX-46 06/80.

Strona internetowa: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

WPROWADZENIE

W celu ułatwienia wykorzystywania Wiążących Reguł Korporacyjnych (BCR) przez korporację (grupę) do prowadzenia przez nią transgranicznego przekazywania danych z UE do organizacji do niej należących, Grupa Robocza Artykułu 29 opracowała następującą tabelę:

- wyjaśniającą wymaganą zawartość BCR, określoną odrębnie w dokumentach WP 74[1] oraz WP 108[2],

- dokonującą rozróżnienia między tym, co musi być uwzględnione w BCR i tym, co musi być przedstawione organom ochrony danych we wniosku dotyczącym BCR (dokument WP 133[3]),

- podającą odniesienia do konkretnych tekstów źródłowych w dokumentach WP 74[4] oraz WP 108[5] w celu uzyskania szczegółowych informacji, oraz

- podającą wyjaśnienia/komentarze do poszczególnych zasad.

---

[1] Dokument Roboczy WP 74: Przekazywanie danych osobowych do państw trzecich: zastosowanie artykułu 26 ust. 2 Dyrektywy UE o ochronie danych w odniesieniu do Wiążących Reguł Korporacyjnych dla transgranicznego przekazywania danych, przyjęty 3 czerwca 2003 r.
http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2003_en.htm

[2] Dokument Roboczy WP 108: Ustanowienie wzorcowej listy kontrolnej dla wniosków o zatwierdzenie Wiążących Reguł Korporacyjnych, przyjęty 14 kwietnia 2005 r.,
http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm

[3] Dokument Roboczy WP 133: Rekomendacja 1/2007 w sprawie standardowego wniosku o zatwierdzenie Wiążących Reguł Korporacyjnych dla transgranicznego przekazywania danych osobowych

[4] Patrz przypis 1

[5] Patrz przypis 2

KRYTERIA AKCEPTACJI BCR	W BCR	W formularzu	Teksty źródłowe	Komentarze
1 – WIĄŻĄCY CHARAKTER				
WEWNĘTRZNIE				
1.1 Obowiązek przestrzegania BCR	TAK	TAK	WP74 pkt 3.3.1 (str. 10-11) + WP 108 pkt 5.3 do 5.9 (str. 5)	BCR muszą jasno nakładać na wszystkich członków Grupy i pracowników obowiązek przestrzegania BCR.
1.2 Wyjaśnienie wiążącego charakteru reguł względem członków grupy i pracowników	NIE	TAK	WP74 pkt 3.3.1 (str. 10-11) + WP 108 pkt 5.3 to 5.9 (str. 5)	Grupa będzie zobowiązana wyjaśnić w formularzu, w jaki sposób zapewnia wiążący charakter reguł: i) Pomiędzy spółkami/jednostkami w obrębie grupy przez jeden lub więcej środków: -umowa wewnątrzgrupowa, -zobowiązania jednostronne, -regulacje wewnętrzne, -polityka grupy, i in. ii) Względem pracowników przez jeden lub więcej środków: -odrębna indywidualna umowa/zobowiązanie przewidująca możliwość sankcji, -klauzula w umowie o pracę przewidująca możliwość sankcji, -polityka wewnętrzna przewidująca możliwość sankcji, lub -umowy zbiorowe przewidujące możliwość sankcji,
ZEWNĘTRZNIE				
1.3 Stworzenie uprawnień osób trzecich dla osób, których dane dotyczą, w tym możliwości złożenia skargi do właściwego organu ochrony danych i do sądu (wybór jurysdykcji: sąd właściwy dla przesyłającego dane/instytucje UE/państwo członkowskie UE odpowiedzialne za ochronę danych)	TAK	TAK	WP 74 pkt 3.3.2. (str. 11-13) i pkt 5.5.1. (str. 18) oraz pkt 5.6 (str. 19) + WP108 pkt 5.12 do 5.14, pkt 5.16, pkt 5.20 (str. 6)	**BCR muszą umożliwiać osobom, których dane dotyczą, wykonywanie uprawnień jako osobom trzecim. Uprawnienia powinny obejmować zadośćuczynienie za wszelkie pogwałcenia zagwarantowanych praw oraz prawo do otrzymania odszkodowania (patrz art. 22 i 23 dyrektywy).**

1.4 Przedsiębiorstwo przyjmuje odpowiedzialność odpowiedzialność za ewentualne odszkodowanie i zadośćuczynienie za pogwałcenie BCR.	TAK	TAK	WP 74 pkt 3.3.1, ust. 5-6 (str. 11) i pkt 5.5.2 (str. 18-19) + WP108 pkt 5.17 (str. 6)	BCR muszą obejmować spoczywający na instytucjach UE lub państwie członkowskim odpowiedzialnym za ochronę danych obowiązek przyjęcia odpowiedzialności za działania innych członków grupy objętych BCR poza UE, i zgodę na podjęcie działań niezbędnych dla zadośćuczynienia pogwałceniu przez nich BCR oraz wypłaceniu wszelkich związanych z nim odszkodowań. BCR muszą również stanowić, że w przypadku pogwałcenia BCR przez członka grupy znajdującego się poza obszarem UE, sprawa będzie podlegać jurysdykcji sądów i innych kompetentnych organów w UE, zaś osoba, której dane dotyczą będzie miała prawo wystąpić o odszkodowanie przeciwko członkowi grupy, który przyjął odpowiedzialność, tak, jakby naruszenie reguł miało miejsce w państwie członkowskim, w którym ma on siedzibę, a nie poza obszarem UE. Jeśli w przypadku niektórych grup o szczególnej strukturze korporacyjnej nie jest możliwe wyznaczenie określonej jednostki, która weźmie na siebie całą odpowiedzialność za wszelkie pogwałcenia BCR mające miejsce poza obszarem UE, organy ochrony danych mogą przyjąć inne mechanizmy nakładania odpowiedzialności, oparte na poszczególnych przypadkach, jeśli zachodzi wystarczająca pewność, że prawa osób, których dane dotyczą będą możliwe do wykonania, i że ich egzekwowanie nie będzie utrudnione. Takimi rozwiązaniami alternatywnymi są mechanizm dzielenia odpowiedzialności pomiędzy jednostki przesyłające i odbierające dane, uwzględniony we Wzorcowych Klauzulach Umownych UE 2001/497/WE z dnia 15 czerwca 2001 lub program przyjmowania odpowiedzialności oparty na analizie prawnej sytuacji firmy, opisany we Wzorcowych Klauzulach Umownych UE 2004/915/WE z dnia 27 grudnia 2004. Ostatnią możliwością, stworzoną z myślą o przekazywaniu danych od administratorów do przetwarzających dane, jest mechanizm odpowiedzialności opisany we Wzorcowych Klauzulach Umownych 2002/16/WE z dnia 27 grudnia 2001.
1.5 Firma posiada odpowiednie aktywa.	NIE	TAK	WP 74 pkt 5.5.2. §2 (str. 18) + WP108 pkt	Formularz musi zawierać potwierdzenie, że jednostka, która przyjęła odpowiedzialność za działania innych członków grupy

			5.17. (str. 6)	podlegającej BCR , znajdujących się poza obszarem UE posiada aktywa wystarczające do zapłacenia odszkodowania za szkody wynikające z pogwałcenia BCR.
1.6 Ciężar dowodu spoczywa na firmie, nie na obywatelu.	TAK	TAK	WP 74 pkt 5.5.2. § 6 i 7 (str. 19) + WP108 pkt 5.19 (str. 6)	BCR muszą stanowić, że na jednostce, która zaakceptowała odpowiedzialność, będzie również spoczywał ciężar dowodu – będzie musiała wykazać, że członek grupy znajdujący się poza obszarem UE nie jest odpowiedzialny za pogwałcenie reguł, w wyniku którego osoba, której dane dotyczą domaga się odszkodowania. Jeśli podmiot, który zaakceptował odpowiedzialność jest w stanie udowodnić, że członek grupy znajdujący się poza obszarem UE nie jest odpowiedzialny za zaistnienie danej sytuacji, może zostać zwolniony z odpowiedzialności.
1.7 Łatwy dostęp osób, których dane dotyczą do BCR, w szczególności do informacji o uprawnieniach osób trzecich dla korzystających z nich osób, których dane dotyczą.	TAK	NIE	WP74 pkt 5.7 (str. 19)	BCR muszą dawać każdej osobie, której dane dotyczą, prawo łatwego dostępu do BCR. Wszystkie osoby, których dane dotyczą, korzystające z uprawnień osób trzecich również powinny mieć łatwy dostęp do tej klauzuli. Na przykład, BCR mogą stanowić, że reguły zostaną opublikowane w internecie lub intranecie (jeśli osoby, których dane dotyczą, są pracownikami firmy).
2 - EFEKTYWNOŚĆ				
2.1 Istnienie odpowiedniego programu szkoleniowego	TAK	TAK	WP 74 pkt 5.1. (str. 16) + WP 108 pkt 5.8-5.9. (str. 5)	BCR muszą zapewniać zorganizowanie odpowiedniego szkolenia dotyczącego reguł dla pracowników posiadających stały lub regularny dostęp do danych osobowych, uczestniczących w ich zbieraniu lub tworzeniu narzędzi służących do ich przetwarzania. Organy ochrony danych oceniające BCR mogą poprosić o przedstawienie przykładów i objaśnienie programu szkoleniowego podczas rozpatrywania wniosku, program szkoleniowy powinien być opisany we wniosku.
2.2 Istnienie procedury rozpatrywania skarg w BCR	TAK	TAK	WP 74 pkt 5.3. (str. 17) + WP 108 pkt 5.15	BCR muszą ustanawiać wewnętrzną procedurę rozpatrywania skarg. Każda osoba, której dane dotyczą powinna móc złożyć

			i 5.18 (str. 6)	skargę, że jeden z członków grupy nie stosuje się do reguł. Skargi winny być rozpatrywane przez ściśle określony departament lub osobę o odpowiednim poziomie niezależności w sprawowaniu funkcji. Formularz musi opisywać sposób informowania osoby, której dane dotyczą o praktycznych krokach podejmowanych w systemie skarg, na przykład: - gdzie złożyć skargę, - w jakiej postaci, - termin odpowiedzi, - konsekwencje w przypadku odrzucenia skargi, - konsekwencje w przypadku uznania skargi za zasadną, - konsekwencje w przypadku, jeśli osoba, której dane dotyczą, nie jest usatysfakcjonowana odpowiedzią (prawo wniesienia sprawy do sądu/organu ochrony danych)

2.3 Istnienie programu audytów obejmującego BCR	TAK	TAK	WP 74 pkt 5.2. (str. 16) + WP 108 pkt 6 (str. 7)	BCR muszą zobowiązywać do regularnego przeprowadzania audytów ochrony danych (przez akredytowanych audytorów wewnętrznych lub zewnętrznych), również na żądanie Administratora Bezpieczeństwa Informacji (lub innego kompetentnego pracownika firmy). BCR muszą zapewnić objęcie programem audytów wszystkich aspektów reguł oraz podejmowanie działań naprawczych. Ponadto BCR muszą zagwarantować przedstawienie wyników audytu Administratorowi Bezpieczeństwa Informacji oraz zarządowi spółki-matki. BCR muszą dawać organom ochrony danych dostęp na żądanie do wyników audytu i możliwość samodzielnego wykonywania kontroli w zakresie ochrony danych, gdy jest to wymagane. Formularz będzie zawierać opis systemu audytów, na przykład : - która jednostka (departament w obrębie grupy) ustala plan/program audytów, - która jednostka przeprowadza audyt, - czas audytu (regularnie lub na żądanie Administratora Bezpieczeństwa Informacji) - zasięg audytu (na przykład aplikacje, systemy informatyczne, bazy danych, w których przetwarzane są dane osobowe, dalsze przekazywanie danych, podejmowane decyzje dotyczące konfliktów prawa krajowego z BCR, przegląd warunków umów stosowanych przy przekazywaniu danych poza grupę (do innych administratorów), działania naprawcze …) - które jednostki otrzymają wyniki audytów

2.4 Stworzenie sieci Administratorów Bezpieczeństwa Informacji lub pracowników oddelegowanych do zajmowania się skargami oraz nadzorowania i zapewniania zgodności z regułami.	TAK	NIE	WP 74, pkt 5.1 (str. 16) i 5.3 (str. 17)	Zobowiązanie do wyznaczenia pracowników (np. sieci Administratorów Bezpieczeństwa Informacji), którzy mają, z poparciem kierownictwa, nadzorować i zapewniać zgodność z regułami. Krótki opis struktury wewnętrznej, roli i zadań sieci Administratorów Bezpieczeństwa Informacji lub innych podobnych funkcji, utworzonych by zapewnić zgodność z regułami. Na przykład główny Administrator Bezpieczeństwa Informacji doradza zarządowi, współpracuje z organami ochrony danych podczas postępowań, co roku składa sprawozdanie dotyczące zgodności, zapewnia zgodność na poziomie globalnym, zaś Administratorzy Bezpieczeństwa Informacji mogą odpowiadać za rozpatrywanie lokalnych skarg od osób, których dane dotyczą, zgłaszać istotne kwestie głównemu Administratorowi Bezpieczeństwa Informacji i zapewniać zgodność na poziomie lokalnym.
3 – OBOWIĄZEK WSPÓŁPRACY				
3.1 Obowiązek współpracy z organami ochrony danych	TAK	TAK	WP 74 pkt 5.4. (str. 17) + WP108 pkt 5.21 (str. 7)	BCR powinny nakładać na grupę jasno określony obowiązek współpracy z organami ochrony danych, zgody na przeprowadzanie przez nie kontroli i zobowiązanie do zastosowania się do ich zaleceń we wszelkich kwestiach związanych z regułami.
4 – OPIS PRZETWARZANIA I PRZEPŁYWU DANYCH				
4.1 Opis operacji przekazywania danych objętych BCR	TAK	TAK	WP 74 pkt 4.1 ust. 4 (str. 14) + WP 108 pkt 7 (str. 7-8)	BCR muszą zawierać również ogólny opis operacji przekazywania, pozwalający organom ochrony danych na ocenę, czy przetwarzanie danych w państwach trzecich jest odpowiednie, a konkretnie dotyczący: i) rodzaju przekazywanych danych ii) celu przesyłania/przetwarzania iii) przesyłającego/odbiorcy danych w UE i poza nią Niektóre organy ochrony danych mogą wymagać bardziej szczegółowego opisu operacji przekazywania
4.2 Określenie zakresu geograficznego i rzeczowego BCR (rodzaj danych, typ osób,	TAK	TAK	WP 108 pkt 7.1.1 i 7.2 (str. 7 i 8)	BCR powinny wskazywać, czy odnoszą się do: i) wszystkich danych osobowych przekazywanych z UE w

których dane dotyczą, kraje)				ramach grupy CZY, ii) wszelkich operacji przetwarzania danych osobowych prowadzonych w ramach grupy BCR muszą również mieć określony zakres rzeczowy, na przykład odnosić się do danych osobowych dotyczących pracowników, klientów, dostawców i innych stron trzecich w ramach danej działalności biznesowej.
5 – MECHANIZMY ZGŁASZANIA I ZAPISYWANIA ZMIAN				
5.1 Proces aktualizacji BCR	TAK	TAK	WP 74 pkt 4.2. (str. 15) + WP 108 pkt 9 (str. 8-9)	BCR mogą być zmieniane (*na przykład aby odzwierciedlać zmiany obowiązujących przepisów lub struktury firmy*), powinny jednak nakładać obowiązek zgłaszania wszelkich dokonanych zmian wszystkim członkom grupy oraz organom ochrony danych. Zmian w BCR lub liście członków BCR można dokonywać bez konieczności ponownego ubiegania się o autoryzację, pod warunkiem, że: i) Określona osoba prowadzi ciągle aktualizowaną listę członków grupy oraz śledzi i zapisuje wszelkie zmiany reguł i udziela niezbędnych informacji na żądanie osób, których dane dotyczą i organów ochrony danych. ii) Nie przekazuje się danych do nowych członków do momentu ich objęcia przez BCR i zobowiązania do zachowania zgodności. iii) Wszelkie istotne zmiany w BCR lub liście członków zgłaszane są raz w roku organom ochrony danych udzielającym autoryzacji wraz z krótkim wyjaśnieniem przyczyn ich dokonania.
6 – ZABEZPIECZENIE DANYCH OSOBOWYCH				
6.1 Opis polityki prywatności, w tym zasad przekazywania lub dalszego przesyłania danych poza obszar UE.	TAK	TAK	WP 108 pkt 8 (str. 8) + WP74 pkt 3.1, ostatni ustęp i pkt 3.2 w sprawie TBDF (str.	BCR powinny wyjaśniać, jak są w firmie stosowane następujące zasady: i) Przejrzystości i rzetelności ii) Ograniczenia celu

			9)	iii) Jakości danych iv) Bezpieczeństwa – w tym obowiązek zawierania umów ze wszystkimi podwykonawcami/administratorami, określających sposób korzystania z danych i konieczne środki bezpieczeństwa v) Prawa dostępu i poprawiania danych a także sprzeciwu wobec ich przetwarzania vi) Ograniczenia przekazywania lub dalszego przesyłania danych do administratorów nienależących do grupy (członkowie grupy będący administratorami mogą przekazywać dane innym administratorom spoza grupy zlokalizowanym poza obszarem UE pod warunkiem zapewnienia odpowiedniej ochrony na mocy art. 16, 17, 25 i 26 dyrektywy 95/46/WE)
6.2 Lista podmiotów objętych BCR	NIE	TAK	WP 108 pkt 7.1.3 (str. 8)	Patrz także pkt 5.1 w tym dokumencie – obowiązek dla określonej osoby kontaktowej w grupie do prowadzenia ciągle aktualizowanej listy jednostek objętych BCR ora potrzeba informowania organów ochrony danych oraz osoby, której dane dotyczą, o ewentualnych zmianach na liście.
6.3 Potrzeba przejrzystości w wypadku, gdy prawodawstwo krajowe nie pozwala grupie zastosować się do postanowień BCR	TAK	NIE	WP74 pkt 3.3.3. (str. 13-14)	Wyraźne zobowiązanie członków grupy: jeśli będą mieli podstawy sądzić, że odnoszące się do nich prawodawstwo nie pozwala firmie wypełnić zobowiązań nałożonych na nią przez BCR i w istotny sposób wpływa na gwarancje zapewniane przez reguły, bezzwłocznie zawiadomią instytucje europejskie lub państwa członkowskie odpowiedzialne za ochronę danych lub innego odpowiedniego Administratora Bezpieczeństwa Informacji (z wyjątkiem przypadków, w których jest to prawnie zabronione – na przykład kiedy prawo karne nakazuje utrzymanie w tajemnicy dochodzenia prowadzonego przez organy ścigania). Ponadto, zobowiązanie, że w przypadku konfliktu między prawem krajowym a zobowiązaniami nałożonymi przez BCR, instytucje europejskie lub państwa członkowskie odpowiedzialne za ochronę danych lub inny odpowiedni Administrator Bezpieczeństwa Informacji podejmą odpowiedzialną decyzję w sprawie działań, jakie należy podjąć, w razie wątpliwości konsultując ją z kompetentnymi w tej sprawie organami ochrony danych.
6.4 Oświadczenie dotyczące powiązań BCR z	NIE	NIE	B/D	Mimo, że nie jest wymagane przez WP 74 i 108, bardzo

prawem krajowym				przydatne jest określenie powiązań pomiędzy BCR i odpowiednim prawem właściwym. BCR mogą stanowić, że mają zastosowanie niezależnie od lokalnego prawodawstwa odnoszącego się do przetwarzania danych przez firmę, jeśli prawodawstwo lokalne zapewnia wyższy poziom ochrony danych, będzie mieć pierwszeństwo przed BCR. W każdej sytuacji dane muszą być przetwarzane zgodnie z właściwym prawem, na mocy Art. 4 dyrektywy 95/46/WE i odpowiedniego prawodawstwa lokalnego.

Sporządzono w Brukseli, 24 czerwca 2008 r.

W imieniu Grupy Roboczej

Przewodniczący

Alex Türk