Krajowa Konferencja Ochrony Danych Osobowych

IV. Compliance

12. Binding Corpotare Rules w zakresie ochrony danych osobowych i ich wpływ na realizację wymogów ochrony danych osobowych w Polsce.

prelegent

Konrad Czaplicki

JDS Consulting sp. z o.o. sp.k. | ul. Gorzelnicza 9, 04-212 Warszawa

tel. 22 651 60 31 | fax 22 651 60 32 | kom. 501 939 269 | e-mail: office@jds.com.pl | www.jds.com.pl, www.dane-osobowe.com

REGON 141620590 | NIP 1132742035 | KRS 0000315726

Bank Zachodni WBK S.A. 32 Oddział w Warszawie | nr 69 1090 1753 0000 0001 1035 7206

Art. 48 ust. 2 ustawy o ochronie danych osobowych po nowelizacji:

Zgoda Generalnego Inspektora nie jest wymagana, jeżeli administrator danych zapewni odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą, przez:

- **standardowe klauzule umowne** ochrony danych osobowych, zatwierdzone przez Komisję Europejską zgodnie z art. 26 ust. 4 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.Urz. WE L 281 z 23.11.1995, str. 31, z późn. zm.; Dz.Urz. UE Polskie wydanie specjalne, rozdz. 13, t. 15, str. 355, z późn. zm.) lub
- prawnie wiążące reguły lub polityki ochrony danych osobowych, zwane dalej „**wiążącymi regułami korporacyjnymi**”, które zostały zatwierdzone przez Generalnego Inspektora

Wiążące reguły korporacyjne:

- To wewnętrzne regulacje obowiązujące w podmiotach powiązanych kapitałowo (podmioty należące do jednej „grupy”)
- Zasadą takich regulacji jest to, że w sposób zasadniczo jednolity regulują określony obszar biznesowy lub prawny we wszystkich podmiotach powiązanych kapitałowo
- Obszar ten traktujemy nie terytorialnie ale handlowo, a więc w każdym aspekcie działalności podmiotów korporacji, w których odbywa się przetwarzanie danych osobowych

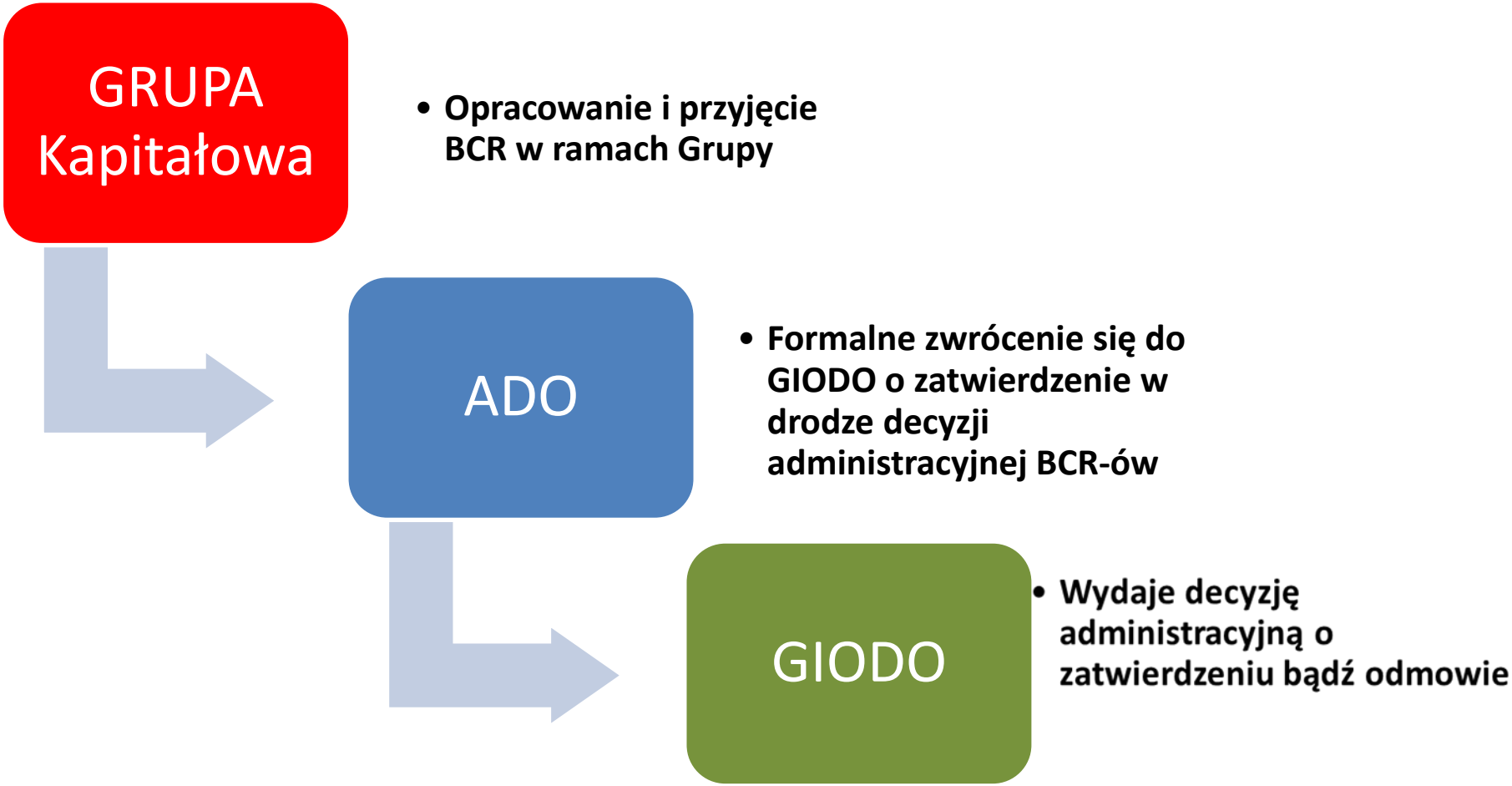
Przykłady wiążących reguł korporacyjnych:

- wewnętrzne kodeksy postępowania (ang. Code of Conduct), np. w zakresie etyki biznesowej, procedur anty-fraudowych, korupcyjnych, z zakresu compliance i polityk zgodności

- standardowe procedury operacyjne (ang. SOP – Standard Operating Procedures) – na przykład dotyczące ochrony informacji, zakupów i zamówień, bezpieczeństwa antywirusowego etc.

BCR istniały i były zawierane w ramach Grup Kapitałowych długo przed nowelizacją ustawy o ochronie danych osobowych!

Tryb postępowania z BCR



JDS Consulting sp. z o.o. sp.k. | ul. Gorzelnicza 9, 04-212 Warszawa

tel. 22 651 60 31 | fax 22 651 60 32 | kom. 501 939 269 | e-mail: office@jds.com.pl | www.jds.com.pl, www.dane-osobowe.com, www.facebook.com/JDS.Consulting.2003

REGON 141620590 | NIP 1132742035 | KRS 0000315726

Bank Zachodni WBK S.A. 32 Oddział w Warszawie | nr 69 1090 1753 0000 0001 1035 7206

Wiążące reguły korporacyjne regulacja ustawowa:

Art. 48

3. Generalny Inspektor **zatwierdza, w drodze decyzji administracyjnej**, wiążące reguły korporacyjne przyjęte w ramach grupy przedsiębiorców do **celów przekazania danych osobowych przez administratora danych** lub podmiot, o którym mowa w art. 31 ust. 1, do należącego do tej samej grupy innego administratora danych lub podmiotu, o którym mowa w art. 31 ust. 1, w państwie trzecim.

4. Generalny Inspektor przed zatwierdzeniem wiążących reguł korporacyjnych **może przeprowadzić konsultacje z właściwymi organami ochrony danych osobowych państw należących do Europejskiego Obszaru Gospodarczego**, na których terytorium mają siedziby przedsiębiorcy należący do grupy, o której mowa w ust. 3, przekazując im niezbędne informacje w tym celu.

5. Generalny Inspektor, wydając decyzję, o której mowa w ust. 3, **uwzględnia wyniki przeprowadzonych konsultacji**, o których mowa w ust. 4, a **jeżeli wiążące reguły korporacyjne były przedmiotem rozstrzygnięcia organu ochrony danych osobowych innego państwa należącego do Europejskiego Obszaru Gospodarczego - może uwzględnić to rozstrzygnięcie**.

Ile czasu potrzeba na przeprocesowanie wiążących reguł korporacyjnych?

Na czas akceptacji ze strony GIODO ma wpływ szereg czynników:

1. **Szybkość wymiany informacji pomiędzy GIODO a zgłaszającym bądź pomiędzy GIODO, a innymi rzecznikami ochrony danych osobowych na terytorium UE**
2. **Okoliczność czy reguły BCR zostały już zaakceptowane i ocenione przez inne organy na terytorium UE**
3. **Zasoby kadrowe**

<u>Uwaga:</u>
Statystycznie najszybciej BCR procedują uprawnione organy w Niemczech i Francji (duża liczba pracowników organów)
Najdłużej Cypr z uwagi na małą liczbę pracowników

Zdarza się że Grupa wybiera przed którym organem w obrębie EOG złoży wniosek o akceptację BCR dla przyspieszenia procesu.

Wiążące reguły korporacyjne:

Warunki które muszą być spełnione ażeby GIODO zaakceptował wiążące reguły korporacyjne (wg. GIODO):

- **Merytoryczne - zasady przetwarzania danych przyjęte przez przedsiębiorcę muszą być zgodne z prawem UE w zakresie ochrony danych osobowych i przestrzegane we wszystkich podmiotach z grupy bez względu na lokalizację (nawet poza EOG),**
- **Tożsame – BCR musza być jednakowe w całej korporacji, co oznacza że żadna spółka oddział w grupie nie może ustalić własnych odmiennych reguł przetwarzania danych osobowych.**

Wiążące reguły korporacyjne - zalety:

- **Możliwość wspólnego kształtowania procesów w Grupie**
- **Standaryzacja procesów i stosowanych środków ochrony wobec danych osobowych**
- **Zatwierdzone BCR przez GIODO uprawniają do transferowania wszelkich danych osobowych, które objęte są postanowieniami tych reguł (tym samym nie trzeba uzyskiwać każdorazowej zgody GIODO bądź innego organu kontrolnego z UE)**

Wiążące reguły korporacyjne – dostrzegane problemy:

- **Długotrwały proces opracowywania, uzgadniania i przyjmowania treści BCR w Grupie, zwłaszcza jeśli Grupa jest liczna**
- **Mała podatność na zmiany i aktualizacje inicjowane przez jeden podmiot z Grupy (zwłaszcza gdy jest to spółka zależna)**
- **W przypadku gdy podmioty dominujące w Grupie zlokalizowane są poza EOG, nierzadko muszą podmieść standard bezpieczeństwa do poziomu europejskiego, co rodzi koszty**
- **Brak możliwości stosowania BCR-ów do transferowania danych poza grupę kapitałową (np. do podwykonawcy)**
- **Organ ds. ochrony danych osobowych (np. GIODO) może odmówić zatwierdzenia BCR wdrożonych w grupie**

Relacje wiążących reguł korporacyjnych do wewnętrznych Polityk bezpieczeństwa wdrożonych u Administratora danych- (naciski Grupy)

Teoretycznie:

Polityki > Wiążące reguły korporacyjne

Faktycznie:

Polityki < Wiążące reguły korporacyjne

Model idealny:

Polityki = Wiążące reguły korporacyjne

Relacje wiążących reguł korporacyjnych do wewnętrznych Polityk bezpieczeństwa wdrożonych u Administratora danych

Różnice w odpowiedzialności podmiotu:

Brak wdrożenia bądź stosowania się do wiążących reguł korporacyjnych:

- **Odpowiedzialność biznesowa ewentualnie majątkowa**

Brak wdrożenia bądź stosowania się do wewnętrznych Polityk bezpieczeństwa:

- **Odpowiedzialność karna, majątkowa, ewentualnie administracyjna**

BCR w ujęciu Grupy Roboczej Artykułu 29 ds. ochrony danych osobowych

Opracowując BCR warto posługiwać się stanowiskiem Grupy Roboczej:

- w dniu 24 czerwca 2008 r. Grupa Robocza Artykułu 29 przyjęła dokumenty robocze w sprawie Wiążących Reguł Korporacyjnych (BCRs), w tym Dokument roboczy ustanawiający tabelę zawierającą elementy i zasady, które mają być uwzględnione w Wiążących Regułach Korporacyjnych **(WP153)** oraz Dokument roboczy w sprawie określenia ram dla struktury Wiążących Reguł Korporacyjnych (**WP154**) ,
- zaś w 2012 roku Grupa Robocza przyjęła Dokument roboczy (**WP195**), w którym zawarto listę kontrolną zapewniającą przedsiębiorcom wytyczne odnośnie tego, jakie kwestie powinny być uwzględnione w BCR dla przetwarzających

BCR w ujęciu Grupy Roboczej Artykułu 29 ds. ochrony danych osobowych

Co powinno zatem znaleźć się w Wiążących Regułach Korporacyjnych (WP153) bądź w wyjaśnieniach składanych wobec organu ochrony danych

- BCR muszą jasno nakładać na wszystkich członków Grupy i pracowników obowiązek przestrzegania BCR.
- Wyjaśnienie wiążącego charakteru reguł względem członków grupy i pracowników (w jaki sposób zapewnione jest przestrzeganie przez wszystkie podmioty z Grupy)
- 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 .
- BCR muszą regulować zasady przejęcia przez przedsiębiorstwo odpowiedzialności za ewentualne odszkodowanie i zadośćuczynienie osobie której dane dotyczą za pogwałcenie BCR przez inny podmiot z grupy.

BCR w ujęciu Grupy Roboczej Artykułu 29 ds. ochrony danych osobowych

Co powinno zatem znaleźć się w Wiążących Regułach Korporacyjnych (WP153) bądź w wyjaśnieniach składanych wobec organu ochrony danych

- 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.
- BCR muszą dawać każdej osobie, której dane dotyczą, prawo łatwego dostępu do BCR np. BCR mogą stanowić, że reguły zostaną opublikowane w Internecie lub intranecie (jeśli osoby, których dane dotyczą, są pracownikami firmy).

BCR w ujęciu Grupy Roboczej Artykułu 29 ds. ochrony danych osobowych

Co powinno zatem znaleźć się w Wiążących Regułach Korporacyjnych (WP153) bądź w wyjaśnieniach składanych wobec organu ochrony danych

- 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
- BCR muszą ustanawiać wewnętrzną procedurę rozpatrywania skarg. Każda osoba, której dane dotyczą powinna móc złożyć 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.
- 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.

BCR w ujęciu Grupy Roboczej Artykułu 29 ds. ochrony danych osobowych

Co powinno zatem znaleźć się w Wiążących Regułach Korporacyjnych (WP153) bądź w wyjaśnieniach składanych wobec organu ochrony danych

- 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
- 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:
    a) rodzaju przekazywanych danych
    b) celu przesyłania/przetwarzania
    c) przesyłającego/odbiorcy danych w UE i poza nią

BCR w ujęciu Grupy Roboczej Artykułu 29 ds. ochrony danych osobowych

Co powinno zatem znaleźć się w Wiążących Regułach Korporacyjnych (WP153) bądź w wyjaśnieniach składanych wobec organu ochrony danych

- BCR powinny wskazywać, czy odnoszą się do:

i) wszystkich danych osobowych przekazywanych z UE w 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
- BCR powinny wyjaśniać, jak są w firmie stosowane następujące zasady:

a) Przejrzystości i rzetelności

b) Ograniczenia celu

c) Jakości danych

d) Bezpieczeństwa – w tym obowiązek zawierania umów ze wszystkimi podwykonawcami/administratorami, określających sposób korzystania z danych i konieczne środki bezpieczeństwa

e) Prawa dostępu i poprawiania danych a także sprzeciwu wobec ich przetwarzania

f) 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)

BCR w ujęciu Grupy Roboczej Artykułu 29 ds. ochrony danych osobowych

Co powinno zatem znaleźć się w Wiążących Regułach Korporacyjnych (WP153) bądź w wyjaśnieniach składanych wobec organu ochrony danych

- Lista podmiotów objętych BCR
- 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).
- 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.

Dziękuję za uwagę

KONRAD CZAPLICKI

starszy prawnik

Kierownik Zespołu w Dziale Outsourcingu JDS Consulting sp. z o.o.

k.czaplicki@jds.com.pl