



538/14/PL
WP 212

Opinia 02/2014 w sprawie listy kontrolnej wymogów dla wiążących regul korporacyjnych składanych do krajowych organów ochrony danych w UE oraz transgranicznych zasad ochrony prywatności składanych do pełnomocników APEC odpowiedzialnych za rozliczalność w zakresie transgranicznych zasad ochrony prywatności

Przyjęta w dniu 27 lutego 2014 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 są określone w art. 30 dyrektywy 95/46/WE i art. 15 dyrektywy 2002/58/WE.

Obsługę sekretariatu zapewnia Dykcja C (Prawa Podstawowe i Obywatelstwo Unii Europejskiej) Dykcji 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_pl.htm

Współpraca między ekspertami z Grupy Roboczej Art. 29 i gospodarek APEC w zakresie listy kontrolnej wymogów dla wiążących reguł korporacyjnych składanych do krajowych organów ochrony danych w UE oraz transgranicznych zasad ochrony prywatności składanych do pełnomocników APEC odpowiedzialnych za rozliczalność w zakresie transgranicznych zasad ochrony prywatności

INFORMACJE OGÓLNE

Cel listy kontrolnej

Przedmiotowy dokument ma służyć jako nieoficjalna, praktyczna lista kontrolna dla organizacji składających wnioski o zatwierdzenie wiążących reguł korporacyjnych (BCR) lub certyfikację transgranicznych zasad ochrony prywatności (CBPR). Tym samym ma ona ułatwiać opracowywanie i przyjmowanie polityki ochrony danych osobowych zgodnej z każdym ze wspomnianych systemów.

Celem przedmiotowej listy kontrolnej nie jest osiągnięcie wzajemnego uznania obu systemów. Może ona jednak służyć jako podstawa **podwójnej certyfikacji**. W każdym przypadku polityki ochrony danych realizowane przez międzynarodowe przedsiębiorstwa wnioskujące, które prowadzą działalność zarówno w UE, jak i na obszarach APEC, **podlegają zatwierdzeniu odpowiednio** przez właściwe organy w państwach członkowskich UE oraz w gospodarkach APEC zgodnie z mającymi zastosowanie procedurami zatwierdzania.

Kontekst

Eksperci z Grupy Roboczej Art. 29 organów ochrony danych w UE (zwanej dalej „Grupą Roboczą Art. 29”)¹ oraz gospodarek uczestniczących z podgrupy ds. prywatności danych APEC opracowali praktyczne narzędzie służące przyporządkowaniu odpowiednich wymogów BCR i CBPR (zwane dalej „listą kontrolną”)².

Przedmiotowa lista kontrolna stanowi jeden dokument zawierający wykaz głównych elementów zasadniczo wymaganych przez krajowe organy ochrony danych w UE (zwane dalej „organami ochrony danych”) z jednej strony oraz przez odpowiednie organy w gospodarkach APEC z drugiej strony, w odniesieniu do polityk ochrony prywatności przedkładanych do zatwierdzenia jako BCR przez krajowe organy ochrony danych w UE zgodnie z przepisami o ochronie danych obowiązującymi w państwach członkowskich UE lub jako CBPR zgodnie z przepisami obowiązującymi w gospodarkach APEC.

¹ Grupę Roboczą Art. 29 ustanowiono na mocy 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. W jej skład wchodzi: przedstawiciel organu nadzorczego (organów nadzorczych) wskazanego (wskazanych) przez każde państwo członkowskie UE, przedstawiciel Europejskiego Inspektora Ochrony Danych oraz przedstawiciel Komisji Europejskiej. Grupa posiada status organu doradczego i jest niezależna.

² W przyszłości wkład w prace APEC i Grupy Roboczej Art. 29 mogą wnieść przedstawiciele przemysłu i społeczeństwa obywatelskiego zgodnie z mechanizmami zaangażowania zainteresowanych stron w ramach APEC i mechanizmami konsultacji Grupy Roboczej Art. 29.

Urzednicy wyzszege szczebla APEC zatwierdzili przedmiotowa listę kontrolna podczas posiedzenia, które miało miejsce w dniach 27–28 lutego 2014 r., a Grupa Robocza Art. 29 przyjęła opinię/dokument roboczy w sprawie tej listy podczas jej posiedzenia plenarnego, które odbyło się w dniach 26–27 lutego 2014 r.

Struktura listy kontrolnej

W odniesieniu do wszystkich podstawowych zasad i wymogów wspomnianych systemów przedmiotowa lista kontrolna obejmuje:

- „**pakiet wspólny**” opisujący główne elementy, które są wspólne dla BCR i CBPR lub są do nich podobne;
- „**pakiety dodatkowe**” przedstawiające główne różnice między tymi systemami oraz elementy dodatkowe, charakterystyczne dla BCR z jednej strony i CBPR z drugiej.

Chociaż wspólny pakiet zawiera pewne części wspólne zarówno między elementami obowiązkowymi systemu CBPR, jak i BCR, ani uzyskanie certyfikacji CBPR od uznanego pełnomocnika APEC odpowiedzialnego za rozliczalność, ani zatwierdzenie BCR przez krajowy organ ochrony danych w UE nie jest samo w sobie wystarczające. Ponadto organizacja składająca wniosek o zatwierdzenie swoich BCR przez krajowy organ ochrony danych **musi również uwzględnić** elementy zawarte w pakiecie dodatkowym dotyczącym BCR, a organizacja składająca wniosek o uzyskanie certyfikacji swoich CBPR przeprowadzanej przez pełnomocnika APEC odpowiedzialnego za rozliczalność **musi również uwzględnić** elementy wymienione w pakiecie dodatkowym dotyczącym CBPR.

**LISTA KONTROLNA WYMOGÓW DLA WIĄŻĄCYCH REGUŁ
KORPORACYJNYCH SKŁADANYCH DO KRAJOWYCH ORGANÓW
OCHRONY DANYCH W UE ORAZ TRANSGRANICZNYCH ZASAD
OCHRONY PRYWATNOŚCI SKŁADANYCH DO PEŁNOMOCNIKÓW
APEC ODPOWIEDZIALNYCH ZA ROZLICZALNOŚĆ W ZAKRESIE
TRANSGRANICZNYCH ZASAD OCHRONY PRYWATNOŚCI**

SPIS TREŚCI

Wprowadzenie.....	7
Cel i struktura.....	7
Zakres stosowania	9
Lista kontrolna wymogów BCR i CBPR dotyczących ochrony danych osobowych i prywatności.....	12
1. Cel zasad organizacji dotyczących ochrony danych osobowych i prywatności.....	12
2. Zakres stosowania zasad organizacji dotyczących ochrony danych osobowych i prywatności	14
3. Możliwe do wyegzekwowania zobowiązanie w ramach organizacji.....	16
4. Środki sądowe dotyczące osób, których dane dotyczą, oraz prawa beneficjenta będącego osobą trzecią.....	19
5. Odpowiedzialność.....	21
6. Możliwe do wyegzekwowania zobowiązania dotyczące przekazywania danych osobom trzecim	23
7. Stosunki z przetwarzającymi będącymi członkami grupy	26
8. Ograniczenia dotyczące przekazywania danych i dalszego przekazywania danych zewnętrznym przetwarzającym i administratorom danych (niebędącym członkami grupy)	29
9. Definicje.....	33
10. Gromadzenie, przetwarzanie i wykorzystywanie danych osobowych.....	34
11. Jakość i proporcjonalność danych/integralność danych	35
12. Podstawy przetwarzania danych osobowych.....	36
13. Dane sensytywne.....	40
14. Przezrystość i prawo do informacji/powiadomienia	42
15. Prawo dostępu, prawo do sprostowania, usunięcia lub zablokowania danych/dostępu do danych i prawo do korekty danych	45
16. Prawo sprzeciwu/wybór	48
17. Zautomatyzowane decyzje indywidualne.....	51

18. Bezpieczeństwo i poufność	52
19. Program szkoleń	54
20. Monitorowanie i program audytów	55
21. Zgodność i nadzorowanie zgodności.....	57
22. Wewnętrzne mechanizmy wnoszenia skarg.....	59
23. Aktualizacje zasad organizacji dotyczących ochrony danych osobowych i prywatności	60
24. Działania w przypadku ryzyka uniemożliwienia przez lokalne prawodawstwo zachowania zgodności z zasadami organizacji dotyczącymi ochrony danych osobowych i prywatności oraz w przypadku wniosków o udzielenie dostępu składanych przez organy ścigania	62
25. Wzajemna pomoc i współpraca z krajowymi organami ochrony danych w UE/organami egzekwowania ochrony prywatności APEC	64
26. Związek między przepisami prawa lokalnego i zasadami organizacji dotyczącymi ochrony danych osobowych i prywatności.....	65
27. Przepisy końcowe	67
Dodatki.....	68
Dodatek 1. Dokumenty składane przez organizację ubiegającą się o zatwierdzenie jej BCR przez krajowe organy ochrony danych w UE oraz przez organizację ubiegającą się o uzyskanie certyfikacji jej CBPR przeprowadzanej przez pełnomocników APEC odpowiedzialnych za rozliczalność.....	69

Wprowadzenie

W niniejszym dokumencie (zwanym dalej „listą kontrolną”) określono wymogi wspólne zarówno dla wiążących reguł korporacyjnych (zwanych dalej „BCR”), zatwierdzanych zazwyczaj przez krajowe organy ochrony danych w Unii Europejskiej (zwanej dalej „UE”) w odniesieniu do przekazywania danych osobowych poza UE, jednak w obrębie grupy przedsiębiorstw, jak i dla systemu transgranicznych zasad ochrony prywatności (zwanych dalej „CBPR”) w ramach Współpracy Gospodarczej Azji i Pacyfiku (zwanej dalej „APEC”) lub wymogi podobne do BCR lub CBPR.

W przedmiotowej liście kontrolnej określono również dodatkowe elementy wymagane do zatwierdzania BCR i certyfikacji CBPR w kontekście przeglądu procedury zatwierdzania i zapewniania zgodności przeprowadzanej zarówno przez krajowe organy ochrony danych w UE (zwane dalej „organami ochrony danych”), jak i przez uznanych pełnomocników APEC odpowiedzialnych za rozliczalność w zakresie CBPR. Wymogi określone w ramach tej listy nie naruszają procedury indywidualnego zatwierdzania BCR przez krajowe organy ochrony danych zgodnie z przepisami UE o ochronie danych ani procedury certyfikacji CBPR przeprowadzanej przez uznanych pełnomocników APEC odpowiedzialnych za rozliczalność w zakresie CBPR (zwanym dalej „pełnomocnikami APEC odpowiedzialnymi za rozliczalność”). Ponadto wymogi te pozostają bez uszczerbku dla egzekwowania przepisów przez stosowne organy nadzorcze lub organy ścigania.

Przedmiotowa lista kontrolna niekoniecznie stanowi kompleksową analizę wszystkich elementów BCR i CBPR ani też nie zapewnia jedyne sposoby przyporządkowania tych dwóch systemów; ponadto nie powinna ona być postrzegana jako porada prawna ani interpretowana jako oficjalne stanowisko którejkolwiek organizacji, która wzięła udział w jej opracowywaniu.

Cel i struktura

Celem przedmiotowej listy kontrolnej jest ułatwienie wdrażania przez organizację zasad dotyczących ochrony danych osobowych i prywatności, aby tym samym ułatwiać zapewnianie zgodności z wymogami w zakresie BCR i CBPR. Dokument ten ma stanowić praktyczną listę kontrolną dla organizacji, które chcą opracować i wdrożyć politykę ochrony prywatności i zamierzają jednocześnie złożyć wniosek o zatwierdzenie BCR przez krajowe organy ochrony danych oraz o uzyskanie certyfikacji CBPR przeprowadzanej przez pełnomocnika APEC odpowiedzialnego za rozliczalność.

Przedmiotowa lista kontrolna ma stanowić narzędzie porównawcze przeznaczone do stosowania przez organizacje rozważające złożenie wniosku o zatwierdzenie BCR przez krajowe organy ochrony danych w UE oraz o uzyskanie certyfikacji CBPR przeprowadzanej przez pełnomocnika APEC odpowiedzialnego za rozliczalność, tj. organizacje pragnące uzyskać podwójną certyfikację. W ramach jednego dokumentu porównano wymogi BCR i CBPR, aby ułatwić organizacjom sformułowanie zasad ochrony danych osobowych i prywatności w celu spełnienia wymogów obu systemów i zastosowania wspomnianych zasad ochrony danych osobowych i prywatności do jej podmiotów, jednostek zależnych i przedsiębiorstw powiązanych (zwanym

dalej „grupą”). Formalnego stwierdzenia zgodności z którymkolwiek ze wspomnianych systemów można dokonać wyłącznie w oparciu o odpowiednie, uznane procedury mające zastosowanie w każdym systemie zgodnie z wymogami określonymi w mających zastosowanie ramach prawnych.

Przedmiotowa lista kontrolna ma następującą strukturę: każdemu wymogowi zidentyfikowanemu na liście odpowiada pakiet wspólnych lub podobnych elementów wymaganych zarówno w przypadku BCR, jak i CBPR. Następnie przedstawiono dodatkowe pakiety odnoszące się do każdego wymogu BCR i wymogu CBPR, w których wymieniono elementy różniące te dwa systemy. Wspomniane pakiety dodatkowe mogą zawierać również wyjątki i wyjaśnienia wymogów dotyczących tych dwóch systemów. Chociaż we wspólnych pakietach wskazano w pewnym zakresie części wspólne między elementami wymaganymi zarówno w systemie CBPR, jak i BCR, elementy te nie są same w sobie wystarczające, aby pełnomocnik APEC odpowiedzialny za rozliczalność przeprowadził certyfikację CBPR ani by krajowy organ ochrony danych w UE zatwierdził BCR. Ponadto organizacja składająca wniosek o zatwierdzenie swoich BCR przez krajowy organ ochrony danych w UE musi również uwzględnić elementy zawarte w dodatkowych pakietach dotyczących BCR, a organizacja składająca wniosek o uzyskanie certyfikacji swoich CBPR przeprowadzanej przez pełnomocnika APEC odpowiedzialnego za rozliczalność musi uwzględnić również elementy wymienione w dodatkowym pakiecie dotyczącym CBPR.

Należy zauważyć, że między wymogami dotyczącymi zatwierdzania BCR ogólnie nakładanymi przez krajowe organy ochrony danych w UE, w szczególności między wymogami wynikającymi z przepisów UE o ochronie danych a wymogami programowymi dotyczącymi CBPR mogą zachodzić znaczne różnice. Istnieją również różnice między odpowiednimi celami, zakresami stosowania oraz procedurami przeglądu systemów BCR i CBPR. Wskutek takich różnic niektóre wymogi BCR i CBPR nie są w pełni kompatybilne. W związku z tym, aby uniknąć jakiegokolwiek konfliktu z obowiązującymi przepisami, organizacje wnioskujące muszą wyjaśniać w sposób wyczerpujący zakres stosowania swoich zasad ochrony danych osobowych i prywatności. W swoich wnioskach muszą one dokonywać wyraźnego rozróżnienia, w jakich przypadkach będą stosowały przepisy UE o ochronie danych lub wymogi programowe APEC dotyczące CBPR, ponieważ dane osobowe muszą być przetwarzane zgodnie z odpowiednimi wymogami zawartymi w przepisach UE o ochronie danych lub przepisami gospodarek APEC.

Zasady organizacji dotyczące ochrony danych osobowych i prywatności należy dostosowywać tak, aby odzwierciedlały strukturę grupy, do której mają zastosowanie, procesy przetwarzania stosowane przez grupę oraz strategie polityczne i procedury wdrożone przez te organizacje w celu zapewnienia ochrony danych osobowych. Organizacje powinny zatem uwagę mieć na uwadze, że krajowe organy ochrony danych w UE i uznani pełnomocnicy APEC odpowiedzialni za rozliczalność w zakresie CBPR nie będą akceptować zwykłego kopiowania i wklejania treści przedmiotowego dokumentu.

Zakres stosowania

Certyfikacja CBPR ogranicza się do tych organizacji, które są certyfikowane w ramach gospodarki uczestniczącej w systemie CBPR. Zakres stosowania certyfikacji CBPR danej organizacji będzie ograniczony do podmiotów, jednostek zależnych i przedsiębiorstw powiązanych wskazanych przez nią we wniosku o uzyskanie certyfikacji CBPR.

Każda organizacja, która chce przekazywać dane osobowe z państw członkowskich UE do odbiorców znajdujących się w państwach trzecich, może złożyć wniosek do krajowego organu ochrony danych w UE o zatwierdzenie jej BCR. Zakres stosowania BCR danej organizacji będzie ograniczony do podmiotów, jednostek zależnych i przedsiębiorstw powiązanych wskazanych przez nią we wniosku o zatwierdzenie BCR. Poprawne wdrożenie BCR, po ich zatwierdzeniu, skutkuje zapewnieniem odpowiednich zabezpieczeń w zakresie przekazywania danych przez wskazane podmioty UE wskazanym w ten sam sposób podmiotom, jednostkom zależnym i przedsiębiorstwom powiązanym z państw trzecich (określonym we wniosku organizacji).

Zasady ochrony danych osobowych i prywatności mające zastosowanie do transgranicznego przekazywania danych osobowych, o ile zostaną zatwierdzone zgodnie z odpowiednimi procedurami, mogą osiągnąć status polityki danej organizacji lub grupy w odniesieniu do wszelkich przetwarzanych przez nią danych osobowych, określonej na podstawie jej BCR zatwierdzonych przez krajowe organy ochrony danych w UE oraz certyfikacji CBPR przeprowadzonej przez pełnomocników APEC odpowiedzialnych za rozliczalność. W przypadku przetwarzania³ danych osobowych w UE⁴, zastosowanie mają również wymogi zawarte w przepisach UE o ochronie danych. W przypadkach dotyczących przetwarzania danych w gospodarce APEC, zastosowanie mają również przepisy odpowiedniej jurysdykcji.

Podstawę niniejszej listy kontrolnej stanowią następujące dokumenty:

UE:

- dyrektywa 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, zwana dalej „**dyrektywą 95/46**”;

³ Pojęcie przetwarzanie oznacza przechowywanie oraz każdą operację lub zestaw operacji dokonywanych na danych osobowych, jak np. gromadzenie, rejestracja, porządkowanie, adaptacja lub modyfikacja, odzyskiwanie, konsultowanie, wykorzystywanie, ujawnianie poprzez przekazanie, rozpowszechnianie lub udostępnianie w inny sposób, zestawianie lub kompilowanie, blokowanie, usuwanie lub niszczenie (zob. art. 2 lit. b) dyrektywy 95/46/WE).

⁴ Krajowe przepisy państw członkowskich UE o ochronie danych mają zastosowanie do przetwarzania danych osobowych (w tym do przechowywania wówczas gdy a) przetwarzanie danych odbywa się w kontekście prowadzenia przed administratorem danych działalności gospodarczej **na terytorium** państwa członkowskiego; c) administrator danych **nie prowadzi działalności gospodarczej na terytorium UE**, a do celów przetwarzania danych osobowych wykorzystuje środki, zarówno zautomatyzowane, jak i inne, znajdujące się w UE, o ile środki te nie są wykorzystywane wyłącznie do celów tranzytu przez terytorium UE; b) administrator danych nie prowadzi działalności gospodarczej na terytorium UE, lecz w miejscu, gdzie prawo krajowe państwa członkowskiego obowiązuje na mocy międzynarodowego prawa publicznego (zob. art. 4 ust. 1 dyrektywy 95/46/WE).

- krajowe przepisy wdrażające dyrektywę 95/46/WE;
- dokument roboczy: „Przekazywanie danych osobowych do państw trzecich: stosowanie art. 26 ust. 2 dyrektywy UE o ochronie danych do wiążących reguł korporacyjnych w odniesieniu do międzynarodowego przekazywania danych (WP74)” [*Working document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers* (WP74)], przyjęty przez Grupę Roboczą Art. 29 w dniu 3 czerwca 2003 r., zwany dalej „**WP74**”;
- dokument roboczy ustanawiający wzór wniosku o zatwierdzenie wiążących reguł korporacyjnych mającego formę listy kontrolnej (WP108) [*Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules* (WP108)], przyjęty przez Grupę Roboczą Art. 29 w dniu 3 czerwca 2003 r., zwany dalej „**WP108**”;
- zalecenie 1/2007 w sprawie standardowego wniosku o zatwierdzenie wiążących reguł korporacyjnych w odniesieniu do przekazywania danych osobowych (WP133) [*Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data* (WP133)], przyjęte przez Grupę Roboczą Art. 29 w dniu 10 stycznia 2007 r., zwane dalej „**WP133**”;
- dokument roboczy ustanawiający tabelę zawierającą elementy i zasady, które można odnaleźć w wiążących regułach korporacyjnych (WP153) [*Working document setting up a table with the elements and principles to be found in Binding Corporate Rules* (WP153)], przyjęty przez Grupę Roboczą Art. 29 w dniu 24 czerwca 2008 r., zwany dalej „**WP153**”;
- dokument roboczy ustanawiający ramy dla struktury wiążących reguł korporacyjnych (WP154) [*Working document setting up a framework for the structure of Binding Corporate Rules* (WP154)], przyjęty przez Grupę Roboczą Art. 29 w dniu 24 czerwca 2008 r., zwany dalej „**WP154**”;
- dokument roboczy w sprawie najczęściej zadawanych pytań dotyczących wiążących reguł korporacyjnych (WP155) [*Working document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules* (WP155)], przyjęty przez Grupę Roboczą Art. 29 w dniu 24 czerwca 2008 r., ostatnio zmieniony i przyjęty w dniu 8 kwietnia 2009 r., zwany dalej „**WP155**”.

APEC:

- ramowe zasady prywatności APEC [*APEC Privacy Framework*], zwane dalej „**ramowymi zasadami prywatności**”;
- system transgranicznych zasad ochrony prywatności, strategię polityczną, zasady i wytyczne APEC [*APEC Cross-Border Privacy Rules System, Policies, Rules and Guidelines*], zwane dalej „**strategiami politycznymi, zasadami i wytycznymi**”;

- porozumienie APEC dotyczące współpracy w zakresie transgranicznego egzekwowania ochrony prywatności) [*APEC Cooperation Arrangement for Cross-Border Privacy Enforcement*], zwane dalej „**CPEA**”;
- wzór powiadomienia o zamiarze uczestniczenia w systemie transgranicznych zasad ochrony prywatności APEC [*Template Notice of Intent to Participate in the APEC Cross-Border Privacy Rules System*], zwany dalej „**wzorem powiadomienia o zamiarze**”;
- wniosek o uznanie pełnomocnika APEC odpowiedzialnego za rozliczalność [*Accountability Agent APEC Recognition Application*], zwany dalej „**wnioskiem o uznanie**”;
- kwestionariusz wstępny dotyczący systemu transgranicznych zasad ochrony prywatności APEC [*APEC Cross-Border Privacy Rules System Intake Questionnaire*], zwany dalej „**kwestionariuszem wstępnym**”;
- wymogi programowe dotyczące systemu transgranicznych zasad ochrony prywatności APEC [*APEC Cross-Border Privacy Rules System Program Requirements*], zwane dalej „**wymogami programowymi**”.

Lista kontrolna wymogów BCR i CBPR dotyczących ochrony danych osobowych i prywatności

1. Cel zasad organizacji dotyczących ochrony danych osobowych i prywatności

Elementy wspólne wymagane zarówno do zatwierdzenia BCR, jak i certyfikacji CBPR

Zasady organizacji dotyczące ochrony danych osobowych i prywatności powinny:

- zapewniać odpowiednią ochronę w zakresie przekazywania i przetwarzania danych osobowych przez grupę, wymaganą w ramach procesów zatwierdzenia BCR i certyfikacji CBPR[5]; oraz
- stanowić egzekwowalne zobowiązanie organizacji do zapewnienia zgodności z zasadami ochrony danych osobowych i prywatności[6] (zob. sekcja 3 i 21 listy kontrolnej);
- zawierać odniesienia do obowiązujących przepisów o ochronie danych[7].

Elementy dodatkowe wymagane do zatwierdzenia BCR	Elementy dodatkowe wymagane do certyfikacji CBPR
Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą określać wyraźne zobowiązanie wszystkich członków grupy i pracowników do interpretowania i przestrzegania zasad ochrony danych osobowych i prywatności danej organizacji zgodnie z obowiązującymi przepisami[8].	<p>W przypadku gdy zakres krajowych wymogów prawnych wykracza poza oczekiwania określone w ramach systemu CBPR, w dalszym ciągu w pełnym zakresie stosuje się wspomniane krajowe przepisy ustawowe i wykonawcze.</p> <p>W przypadku gdy zakres wymogów systemu CBPR wykracza poza zakres wymogów krajowych przepisów ustawowych i wykonawczych, organizacja będzie musiała dobrowolnie spełnić takie wymogi dodatkowe, aby uczestniczyć w systemie. Organy egzekwowania ochrony prywatności w danej gospodarce powinny jednak mieć możliwość podejmowania działań w zakresie egzekwowania ochrony na mocy obowiązujących przepisów ustawowych i wykonawczych, które skutkują zapewnieniem ochrony danych osobowych zgodnie z wymogami programowymi CBPR[9] (zob. także pkt 26, związek między przepisami lokalnymi i zasadami organizacji dotyczącymi ochrony danych osobowych i prywatności).</p>

Dokumenty odniesienia

- [5] UE: zob. WP74, pkt 3.1, s. 7–9; APEC: zob. ramowe zasady prywatności, część (iii), zasada I, pkt 14, s. 11.
- [6] UE: zob. WP154, Wprowadzenie, s. 3 oraz WP74, s. 10–14; APEC: zob. strategie polityczne, zasady i wytyczne CBPR, pkt 8, s. 4; wymogi programowe CBPR, pkt 39, 40.
- [7] UE: zob. WP154, Wprowadzenie, s. 3; APEC: zob. wniosek o uznanie, załącznik A, pkt 4, s. 5.
- [8] UE: zob. WP74, pkt 3.3.1, s. 10–11; WP153, pkt 1.1, s. 3.
- [9] APEC: zob. strategie polityczne, zasady i wytyczne, pkt 44, s. 10.

2. Zakres stosowania zasad organizacji dotyczących ochrony danych osobowych i prywatności

Elementy wspólne wymagane zarówno do zatwierdzenia BCR, jak i certyfikacji CBPR

Zasady organizacji dotyczące ochrony danych osobowych i prywatności powinny zawierać opis zakresu ich stosowania, w tym:

- zakres geograficzny (zob. sekcje 4 i 15 przedmiotowej listy kontrolnej)[10];
- zakres przedmiotowy (tj. charakter danych, dane klientów/potencjalnych klientów, pracowników/potencjalnych pracowników, dostawców itd.)([11];
- wykaz podmiotów związanych zasadami organizacji dotyczącymi ochrony danych osobowych i prywatności[12]; oraz
- cele przekazywania lub przetwarzania danych[13].

Elementy dodatkowe wymagane do zatwierdzenia BCR Przetwarzanie publicznie dostępnych danych osobowych podlega wymogom przepisów prawa UE o ochronie danych i nie jest zwolnione ze stosowania BCR. Organizacje, które decydują się na uczestnictwo w systemie BCR, muszą wdrażać polityki i praktyki ochrony prywatności spójnie z wymogami programowymi BCR w odniesieniu do wszelkich danych osobowych przekazywanych w ramach grupy poza Unię Europejską. Chociaż nie wymaga się tego do zatwierdzenia BCR, uczestniczące organizacje mogą stosować takie same polityki i procedury ochrony prywatności do wszystkich danych osobowych przetwarzanych w ramach grupy na skalę światową pod warunkiem zapewnienia zgodności z przepisami prawa UE o ochronie danych w przypadku, gdy dane są przetwarzane w UE.	Elementy dodatkowe wymagane do certyfikacji CBPR Nie dotyczy
Wyjaśnienie zakresu stosowania BCR Nie dotyczy	Wyjaśnienie zakresu stosowania CBPR W niektórych przypadkach zasady organizacji dotyczące ochrony danych osobowych i prywatności mogą nie mieć zastosowania do danych dostępnych publicznie[14].

	<p>Organizacje, które decydują się na uczestnictwo w systemie CBPR, powinny wdrożyć polityki i praktyki ochrony prywatności spójnie z wymogami programowymi CBPR w odniesieniu do wszystkich danych osobowych, które zgromadziły lub otrzymały i które są przedmiotem transgranicznego przekazywania danych do innych uczestniczących gospodarek APEC. Chociaż nie jest to wymagane w ramach systemu CBPR, uczestniczące organizacje zachęca się do stosowania takich samych polityk i procedur ochrony prywatności do wszystkich danych osobowych, które zgromadziły lub otrzymały, nawet jeżeli dane te nie są przedmiotem transgranicznego przekazywania danych lub jeżeli są one przedmiotem takiego przekazywania wyłącznie poza uczestniczące gospodarki APEC^[15].</p>
--	---

Dokumenty odniesienia

- [10] UE: zob. WP153, pkt 4.2 oraz WP108, pkt 7.1 i 7.2, s. 7–8; APEC: zob. kwestionariusz wstępny, pkt (v)–(vi), s. 2–3.
- [11] UE: zob. WP153, pkt 4.2 oraz WP108, pkt 7.1.1 i 7.2, s. 7–8; APEC: zob. kwestionariusz wstępny, pkt (iv), s. 2.
- [12] UE: zob. WP153, pkt 6.2; WP108, pkt 7.1.3, s. 8; APEC: zob. kwestionariusz wstępny, pkt (ii), s. 2.
- [13] UE: zob. WP153, pkt 4.1; WP108, pkt 7.1.2, s. 8; APEC: zob. wymogi programowe CBPR, pyt. 1 lit. b) i 1 lit. c).
- [14] APEC: zob. ramowe zasady prywatności APEC, pkt 11, s. 7.
- [15] APEC: zob. strategie polityczne, zasady i wytyczne, pkt 8, s. 4.

3. Możliwe do wyegzekwowania zobowiązanie w ramach organizacji

Elementy wspólne wymagane zarówno do zatwierdzenia BCR, jak i certyfikacji CBPR

Na wszystkich podmiotach należących do grupy i ubiegających się o zatwierdzenie BCR przez krajowy organ ochrony w UE albo o certyfikację CBPR pełnomocnika APEC odpowiedzialnego za rozliczalność musi spoczywać możliwe do wyegzekwowania zobowiązanie do przestrzegania zasad organizacji dotyczących ochrony danych osobowych i prywatności zgodnie z obowiązującymi przepisami, które w stosownych przypadkach mogą być egzekwowane przez osobę fizyczną/osobę, której dane dotyczą, oraz organ regulacyjny[16].

Elementy dodatkowe wymagane do zatwierdzenia BCR: charakter wiążący w ramach grupy (BCR)	Elementy dodatkowe wymagane do certyfikacji CBPR
<p>Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą stać się prawnie wiążące między podmiotami grupy za pośrednictwem co najmniej jednego z następujących instrumentów[17]:</p> <ul style="list-style-type: none">(i) środków lub zasad prawnie wiążących dla wszystkich członków grupy;(ii) umów między członkami grupy;(iii) jednostronnych oświadczeń składanych przez spółkę dominującą lub zobowiązań przez nią podejmowanych, które są wiążące dla innych członków grupy[18];(iii) włączenia innych środków regulacyjnych, na przykład zobowiązań zawartych w kodeksach ustawowych w ramach określonych ram prawnych;(iv) włączenia zasad organizacji dotyczących ochrony danych i prywatności do podstawowych zasad organizacji w zakresie prowadzenia działalności, w oparciu o odpowiednie strategie polityczne, audyty i sankcje;(v) innych środków[19]. <p>Ponadto należy zapewnić, aby zasady organizacji dotyczące ochrony danych osobowych i prywatności były również prawnie wiążące dla pracowników[20], za</p>	<p>Nie dotyczy</p>

<p>pośrednictwem co najmniej jednego z wymienionych poniżej instrumentów:</p> <ul style="list-style-type: none"> (i) indywidualnej i odrębnej umowy przewidującej sankcje/indywidualnego i odrębnego zobowiązania przewidującego sankcje; (ii) klauzuli w umowie o pracę przewidującej sankcje; (iii) wewnętrznych polityk przewidujących sankcje; (iv) układów zbiorowych przewidujących sankcje. 	
<p>Wyjaśnienie wiążącego charakteru w ramach organizacji (BCR)</p> <p>Nie dotyczy</p>	<p>Wyjaśnienie rozliczalności w ramach organizacji (CBPR)</p> <p>Organizacja musi pozostać rozliczalna poprzez wykazanie, że jej zasady ochrony danych osobowych i prywatności są możliwe do wyegzekwowania za pośrednictwem co najmniej jednego z następujących instrumentów[21]:</p> <ul style="list-style-type: none"> (i) wewnętrznych wytycznych lub polityk; (ii) umów; (iii) zapewnienia zgodności z przepisami ustawowymi i wykonawczymi dotyczącymi danej branży przemysłowej lub sektora; (iv) innych środków. <p>Ponadto organizacja musi wdrożyć procedury szkoleń pracowników w zakresie jej zasad ochrony danych osobowych i prywatności[22].</p>

Dokumenty odniesienia

[16] UE: zob. WP153, pkt 1.1 i 1.2; WP74 pkt 3.3.1, s. 10–11; APEC: zob. wymogi programowe, pyt. 39, s. 24; załączniki A i B.

[17] UE: zob. WP153, pkt 1.2 ppkt (i), s. 3; WP108, pkt 5.6, s. 5.

[18] Należy zauważyć, że w niektórych państwach członkowskich UE zwykle jednostronne oświadczenia mogą nie być uznawane za prawnie wiążące na mocy przepisów prawa cywilnego i administracyjnego. W takim przypadku za prawnie wiążące uznaje się wyłącznie umowy. Organizacja będzie musiała zatem skonsultować się z doradcami lokalnymi, jeżeli zamierza się

powoływać na środki prawne inne niż umowy.

[19] UE: WP74, pkt 3.3.1, s. 10–11; WP153, pkt 1.1, s. 3.

[20] UE: zob. WP74, pkt 3.3.1, s. 10–11; WP153, pkt 1.1, s. 3 oraz pkt 1.2 ppkt (ii), s. 3.

[21] APEC: zob. wymogi programowe, pyt. 39, s. 24; pyt. 46, s. 26; załączniki A i B.

[22] APEC: zob. wymogi programowe, pyt. 44, s. 25–26.

4. Środki sądowe dotyczące osób, których dane dotyczą, oraz prawa beneficjenta będącego osobą trzecią

Elementy wspólne wymagane zarówno do zatwierdzenia BCR, jak i certyfikacji CBPR

Nie dotyczy

Elementy wymagane do zatwierdzenia BCR	Elementy wymagane do certyfikacji CBPR
<p>Zgodnie z zasadami organizacji dotyczącymi ochrony danych osobowych i prywatności uprawnienia do egzekwowania zasad ochrony danych osobowych i prywatności wyraźnie nadaje się osobom, których dane dotyczą, jako beneficjentom będącym osobami trzecimi. Należy w nich określić przejrzyste, dostępne i skuteczne środki sądowe w związku z jakimkolwiek naruszeniem zasad ochrony danych osobowych i prywatności oraz prawa do otrzymania odszkodowania (zob. art. 22 i 23 dyrektywy UE 95/46)[23].</p> <p>Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą zawierać również deklarację potwierdzającą, że osoby, których dane dotyczą, mają prawo wyboru dowolnej z wymienionych poniżej możliwości złożenia skargi:</p> <ul style="list-style-type: none">- w ramach jurysdykcji eksportera danych zlokalizowanego w UE; lub- w ramach jurysdykcji siedziby głównej w UE/członka grupy w UE, któremu powierzono obowiązki; lub- przed właściwymi krajowymi organami ochrony danych w UE. <p>Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą zawierać również zapewnienie, że wszystkie osoby, których dane dotyczą, korzystające z praw beneficjenta będącego osobą trzecią także miały łatwy dostęp do tej klauzuli[24].</p>	<p>Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą zawierać deklarację potwierdzającą, że osoby, których dane dotyczą, mogą je egzekwować za pośrednictwem:</p> <ul style="list-style-type: none">- procesu rozpatrywania skarg administratora danych[25]; lub- procesu rozstrzygania sporów pełnomocnika APEC odpowiedzialnego za rozliczalność[26]. <p>Osoby, których dane dotyczą, muszą również mieć możliwość złożenia skargi bezpośrednio do wspólnego panelu ds. nadzoru przeciwko pełnomocnikowi APEC odpowiedzialnemu za rozliczalność[27].</p> <p>Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą również określać wymóg, zgodnie z którym osoby, których dane dotyczą, mogą składać skargi do pełnomocników APEC odpowiedzialnych za rozliczalność[28].</p> <p>W zależności od gospodarek uczestniczących w systemie CBPR osoby, których dane dotyczą, mogą posiadać niezależne prawo do podejmowania działań, określone w ich lokalnych przepisach o ochronie danych, które może być wykorzystywane do egzekwowania zgodności z CBPR.</p>

Dokumenty odniesienia

[23] UE: zob. WP74, pkt 3.3.2, s. 11–13.

[24] UE: zob. WP153, pkt 1.7, s. 5.

[25] APEC: zob. kwestionariusz wstępny, pyt. 41–43, s. 21–22.

[26] APEC: zob. wniosek o uznanie, załącznik A, pkt 9–10, s. 7.

[27] APEC: zob. strategię polityczne, zasady i wytyczne, pkt 35, s. 9.

[28] APEC: zob. wniosek o uznanie, załącznik A, pkt 9–10, s. 7.

5. Odpowiedzialność

Elementy wspólne wymagane zarówno do zatwierdzenia BCR, jak i certyfikacji CBPR

Zasady organizacji dotyczące ochrony danych osobowych i prywatności zasadniczo muszą stanowić, że odpowiedzialność spoczywa na jednym podmiocie[29].

Elementy dodatkowe wymagane do zatwierdzenia BCR	Elementy dodatkowe wymagane do certyfikacji CBPR
<p>Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą również zawierać zobowiązanie, zgodnie z którym[30]:</p> <ul style="list-style-type: none">- siedziba główna w UE albo członek grupy w UE, któremu powierzono obowiązki, odpowiada za podjęcie odpowiednich kroków i zgadza się na ich podjęcie w celu naprawienia sytuacji wynikającej z działań innych członków grupy mającej siedzibę poza UE oraz do wypłaty odszkodowania za wszelkie szkody powstałe w wyniku naruszenia zasad organizacji dotyczących ochrony danych osobowych i prywatności przez członków grupy;- ciężar dowodu spoczywa na siedzibie głównej w UE lub członku grupy w UE, któremu powierzono obowiązek wykazania, że członek grupy spoza UE nie jest odpowiedzialny za naruszenie, w wyniku którego osoba, której dane dotyczą, dochodzi odszkodowania. <p>Jeżeli siedziba główna w UE lub członek grupy w UE, któremu powierzono obowiązki, mogą udowodnić, że członek grupy spoza UE nie jest odpowiedzialny za wspomniane naruszenie, mogą oni zostać zwolnieni z ponoszenia jakiegokolwiek odpowiedzialności.</p> <p>Jeżeli w przypadku niektórych grup o szczególnych strukturach korporacyjnych nie jest możliwe zobowiązanie określonego podmiotu do poniesienia pełnej odpowiedzialności za jakiegokolwiek naruszenie BCR poza UE, w poszczególnych przypadkach krajowe organy ochrony danych</p>	<p>Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą zawierać również zobowiązanie, zgodnie z którym odpowiedzialność spoczywa na podmiocie, który uzyskał certyfikację CBPR. Nie wyklucza to jednak żadnej dodatkowej odpowiedzialności spoczywającej na jednostkach zależnych/przedsiębiorstwach powiązanych, zgodnie z przepisami lokalnymi, wobec których naruszenie miało miejsce.</p>

<p>mogą zatwierdzić inne mechanizmy odpowiedzialności pod warunkiem zapewnienia wystarczającej gwarancji, iż prawa osób, których dane dotyczą, będą możliwe do wyegzekwowania, a one same nie będą napotykały trudności w ich egzekwowaniu^[31].</p>	
--	--

Dokumenty odniesienia

[29] UE: zob. WP74, pkt 5.5.2, s. 18–19; APEC: zob. kwestionariusz wstępny, pkt (ii), s. 2.

[30] UE: zob. WP74, pkt 5.5.2, s. 18–19.

[31] Takie możliwe systemy odpowiedzialności mogą obejmować mechanizm wspólnej odpowiedzialności między odbierającymi dane a przekazującymi dane przewidziany w standardowych klauzulach umownych UE 2001/497/WE z dnia 15 czerwca 2001 r. lub określenie alternatywnego mechanizmu odpowiedzialności w oparciu o zobowiązania w zakresie należytej staranności, jak określono w standardowych klauzulach umownych UE 2004/915/WE z dnia 27 grudnia 2004 r. Ostatnią możliwością, dotyczącą w szczególności danych przekazywanych między administratorami danych i przetwarzającymi, jest zastosowanie mechanizmu odpowiedzialności przewidzianego w standardowych klauzulach umownych 2002/16/WE z dnia 27 grudnia 2001 r.

6. Możliwe do wyegzekwowania zobowiązania dotyczące przekazywania danych osobom trzecim

Elementy wspólne wymagane zarówno do zatwierdzenia BCR, jak i certyfikacji CBPR

Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą zawierać możliwe do wyegzekwowania zobowiązanie, zgodnie z którym organizacja przekazuje dane wyłącznie osobom trzecim zapewniającym ochronę przetwarzania danych osobowych, oraz wyjaśnienie sposobu, w jaki zasady organizacji dotyczące ochrony danych osobowych i prywatności stają się możliwe do wyegzekwowania wobec takich odbiorców danych w odpowiedniej jurysdykcji[32].

Elementy dodatkowe wymagane do zatwierdzenia BCR	Elementy dodatkowe wymagane do certyfikacji CBPR
<p>Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą zawierać zasady ograniczające przekazywanie i dalsze przekazywanie danych poza grupę oraz zobowiązanie do zapewnienia, aby[33]:</p> <ul style="list-style-type: none">- zewnętrzni przetwarzający z siedzibą w UE lub w państwie uznanym przez Komisję Europejską za zapewniające odpowiedni stopień ochrony byli związani pisemną umową, która stanowi, że przetwarzający działa wyłącznie na polecenie administratora danych i jest odpowiedzialny za wdrażanie odpowiednich środków bezpieczeństwa i poufności;- wszelkie przypadki przekazywania danych zewnętrznym administratorom danych z siedzibą poza UE i w państwie nieuznanym przez Komisję Europejską za zapewniające odpowiedni stopień ochrony były zgodne z przepisami UE dotyczącymi transgranicznego przepływu danych (art. 25–26 dyrektywy 95/46/WE: na przykład wykorzystywanie standardowych klauzul umownych UE zatwierdzonych dokumentem Komisji UE 2001/497/WE lub 2004/915/WE, lub innymi odpowiednimi postanowieniami umownymi zgodnie z art. 25 i 26 dyrektywy UE);	<p>Nie dotyczy</p>

<p>- wszelkie przypadki przekazywania danych zewnętrznym przetwarzającym z siedzibą poza UE były zgodne nie tylko z przepisami dotyczącymi przetwarzających (art. 16–17 dyrektywy 95/45/WE), ale również z przepisami dotyczącymi transgranicznego przepływu danych (art. 25–26 dyrektywy 95/46/WE).</p>	
<p>Wyjaśnienie wiążącego charakteru w odniesieniu do stron trzecich (BCR)</p> <p>Nie dotyczy</p>	<p>Wyjaśnienie rozliczalności w odniesieniu do przekazywania danych osobom trzecim (CBPR)</p> <p>Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą zawierać wyjaśnienie sposobu ochrony danych osobowych podczas wykorzystywania ich przez przetwarzającego, pośrednika, wykonawcę lub innego dostawcę usług. W szczególności muszą one zawierać wymóg, zgodnie z którym:</p> <ul style="list-style-type: none"> - administrator danych jest zobowiązany do wybrania przetwarzającego, pośrednika, wykonawcy lub innego dostawcy usług o wystarczających gwarancjach odnośnie do technicznych środków bezpieczeństwa oraz rozwiązań organizacyjnych, regulujących przetwarzanie danych, oraz do zapewnienia stosowania tych środków i rozwiązań^[34]; - administrator danych zleca przetwarzającemu zapewnienie, aby w szczególności: <ul style="list-style-type: none"> (i) przetwarzający, pośrednik, wykonawca lub inny dostawca usług działali wyłącznie na polecenie administratora danych^[35]; (ii) zasady dotyczące bezpieczeństwa i poufności były obowiązkowe dla przetwarzającego, pośrednika, wykonawcy lub innego

	<p>dostawcy usług^[36].</p> <p>Zasady organizacji dotyczące ochrony danych osobowych i prywatności mogą stać się prawnie wiążące za pośrednictwem co najmniej jednego z następujących instrumentów^[37]:</p> <ul style="list-style-type: none"> (i) wewnętrznych wytycznych lub strategii politycznych; (ii) umów; (iii) zapewnienia zgodności z przepisami ustawowymi i wykonawczymi dotyczącymi danej branży przemysłowej lub sektora; (iv) innych środków.
--	---

Dokumenty odniesienia

[32] UE: zob. WP74, pkt 3.2, s. 9–10; APEC: zob. wymogi programowe, pyt. 39, s. 24; pyt. 46, s. 26; załączniki A i B; kwestionariusz wstępny, pyt. 47, s. 22.

[33] UE: zob. WP153, pkt 6.1 ppkt (vi); WP154, pkt 12, s. 7.

[34] APEC: zob. kwestionariusz wstępny, pyt. 35, s. 15.

[35] APEC: zob. kwestionariusz wstępny, pyt. 47–48, s. 22–23.

[36] APEC: zob. kwestionariusz wstępny, pyt. 35, s. 15–16.

[37] APEC: zob. wymogi programowe, pyt. 39, s. 24; pyt. 46, s. 26; załączniki A i B.

7. Stosunki z przetwarzającymi będącymi członkami grupy

Elementy wspólne wymagane zarówno do zatwierdzenia BCR, jak i certyfikacji CBPR

Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą zawierać wyjaśnienie sposobu ochrony danych osobowych w przypadku, gdy przetwarzający jest członkiem grupy, a w szczególności wymóg, zgodnie z którym[38]:

- administrator danych jest zobowiązany do wybrania przetwarzającego o wystarczających gwarancjach odnośnie do technicznych środków bezpieczeństwa oraz rozwiązań organizacyjnych, regulujących przetwarzanie danych, oraz do zapewnienia stosowania tych środków i rozwiązań[39];
- administrator danych poleca przetwarzającemu zapewnienie w szczególności, aby:
 - przetwarzający działał wyłącznie na polecenie administratora danych[40];
 - zasady dotyczące bezpieczeństwa i poufności były obowiązkowe dla przetwarzającego[41].

Elementy dodatkowe wymagane do zatwierdzenia BCR	Elementy dodatkowe wymagane do certyfikacji CBPR
<p>Zasady organizacji dotyczące ochrony danych i prywatności muszą obejmować zobowiązanie, zgodnie z którym polecenia muszą być przekazywane w formie pisemnych postanowień umownych zgodnie z obowiązującymi przepisami[42].</p>	<p>Jeżeli administrator danych zamierza przekazywać dane osobowe przetwarzającym, pośrednikom, wykonawcom lub innym dostawcom usług, powinien on otrzymać zgodę osoby, której dane dotyczą, lub postąpić z należytą starannością i podjąć właściwe działania mające na celu zapewnienie, aby osoba fizyczna lub organizacja otrzymująca dane chroniła je, przestrzegając zasad organizacji dotyczących ochrony danych osobowych i prywatności[43].</p> <p>W sytuacjach, w których postępowanie z należytą starannością i podjęcie właściwych kroków mających na celu zapewnienie przestrzegania zasad organizacji dotyczących ochrony danych osobowych i prywatności jest niepraktyczne lub niemożliwe, administrator danych musi przedstawić wyjaśnienie i opisać inne środki zastosowane w celu zagwarantowania, że dane mimo wszystko są chronione zgodnie z zasadami ochrony prywatności APEC.</p> <p>Administrator danych może wydawać polecenia[44]:</p>

	<ul style="list-style-type: none"> - za pośrednictwem wewnętrznych wytycznych lub strategii politycznych; lub - za pośrednictwem umów; lub - zapewniając zgodność z przepisami ustawowymi i wykonawczymi dotyczącymi danej branży przemysłowej lub sektora; lub - stosując kodeks lub zasady organu samoregulacyjnego; lub - za pośrednictwem innych środków. <p>Wspomniane uzgodnienia zasadniczo wymagają uwzględnienia przez przetwarzających, pośredników, wykonawców lub innych dostawców usług^[45] odpowiednich środków ochrony spośród następujących możliwości:</p> <ul style="list-style-type: none"> - przestrzegania polityki i praktyk ochrony prywatności zgodnych z APEC, stosowanych przez administratora danych i określonych w oświadczeniu administratora danych o polityce ochrony prywatności; - wdrażania praktyk ochrony prywatności, które są zasadniczo podobne do polityki i praktyk ochrony prywatności stosowanych przez administratora danych, określonych w oświadczeniu administratora danych o polityce ochrony prywatności; - wykonywania poleceń wydawanych przez administratora danych dotyczących sposobu obchodzenia się z danymi osobowymi administratora danych; - nakładania ograniczeń na zlecenie podwykonawstwa, chyba że zleca się je za zgodą administratora danych; - uzyskania certyfikacji CBPR przeprowadzanej przez pełnomocnika APEC odpowiedzialnego za rozliczalność w ich jurysdykcji; <p>Przetwarzający, pośrednicy, wykonawcy lub inni dostawcy usług powiadamiają administratora danych o przypadkach</p>
--	--

	<p>naruszenia prywatności lub bezpieczeństwa danych osobowych administratora danych, w przypadku gdy dowiedzą się o takim naruszeniu[46].</p> <p>Przetwarzający, pośrednicy, wykonawcy lub inni dostawcy usług natychmiast podejmują działania w celu naprawienia/wyeliminowania niedopatrzeń w zakresie bezpieczeństwa, które spowodowały naruszenie prywatności lub bezpieczeństwa[47].</p> <p>Przetwarzający, pośrednicy, wykonawcy lub inni dostawcy usług przedstawiają administratorowi danych samooceny w celu zapewnienia zgodności z poleceniami administratora danych lub uzgodnieniami/umowami[48].</p> <p>Administrator danych przeprowadza regularne kontrole weryfikacyjne lub monitoruje przetwarzających, pośredników, wykonawców lub innych dostawców usług wykorzystujących jego dane osobowe w celu zapewnienia zgodności z jego poleceniami lub uzgodnieniami/umowami[49].</p>
--	--

Dokumenty odniesienia

- [38] UE: zob. dyrektywa 95/46, art. 17 ust. 2; WP154, pkt 11, s. 6–7.
- [39] APEC: zob. kwestionariusz wstępny, pyt. 35, s. 15.
- [40] APEC: zob. kwestionariusz wstępny, pyt. 47–48, s. 22–23.
- [41] APEC: zob. kwestionariusz wstępny, pyt. 35, s. 15–16.
- [42] UE: zob. dyrektywa 95/46, art. 17 ust. 2; WP154, pkt 11, s. 6–7.
- [43] APEC: zob. ramowe zasady prywatności, część (iii), zasada IX, pkt 26, s. 28.
- [44] APEC: zob. kwestionariusz wstępny, pyt. 46, s. 22.
- [45] APEC: zob. kwestionariusz wstępny, pyt. 47, s. 22–23.
- [46] APEC: zob. kwestionariusz wstępny, pyt. 35 lit. d), s. 15.
- [47] APEC: zob. kwestionariusz wstępny, pyt. 35 lit. c), s. 16.
- [48] APEC: zob. kwestionariusz wstępny, pyt. 48, s. 23.
- [49] APEC: zob. kwestionariusz wstępny, pyt. 49, s. 23.

8. Ograniczenia dotyczące przekazywania danych i dalszego przekazywania danych zewnętrznym przetwarzającym i administratorom danych (niebędącym członkami grupy)

Elementy wspólne wymagane zarówno do zatwierdzenia BCR, jak i certyfikacji CBPR

Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą zawierać wymóg, zgodnie z którym wykonawcy otrzymujący dane i przetwarzający je są zobowiązani do ochrony danych osobowych zgodnie z zasadami ochrony danych osobowych i prywatności obowiązującymi w organizacji przekazującej dane[50].

Elementy dodatkowe wymagane do zatwierdzenia BCR	Elementy dodatkowe wymagane do certyfikacji CBPR
<p>Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą również zawierać uzasadnienie środków wprowadzonych w celu ograniczenia przekazywania danych i dalszego przekazywania danych poza grupę oraz zobowiązanie do zapewnienia, aby:</p> <ul style="list-style-type: none"> - zewnątrzni przetwarzający z siedzibą w UE lub w państwie uznanym przez Komisję Europejską za zapewniające odpowiedni stopień ochrony byli związani pisemną umową, która stanowi, że przetwarzający działa wyłącznie na polecenie administratora danych i jest odpowiedzialny za wdrażanie odpowiednich środków bezpieczeństwa i poufności[51]; - wszelkie przypadki przekazywania danych zewnętrznym administratorom danych z siedzibą poza UE lub w państwie nieuznanym przez Komisję Europejską za zapewniające odpowiedni stopień ochrony musiały być zgodne z przepisami UE dotyczącymi transgranicznego przepływu danych (art. 25–26 dyrektywy 95/46/WE: na przykład poprzez wykorzystywanie standardowych klauzul umownych UE zatwierdzonych dokumentem Komisji UE 2001/497/WE lub 2004/915/WE lub innych odpowiednich postanowień 	<p>Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą również zawierać wyjaśnienie sposobu ochrony danych osobowych, podczas wykorzystywania ich przez przetwarzającego, pośrednika, wykonawcę lub innego dostawcę usług. W szczególności muszą one zawierać wymóg, zgodnie z którym:</p> <ul style="list-style-type: none"> - administrator danych jest zobowiązany do wybrania przetwarzającego, pośrednika, wykonawcy lub innego dostawcy usług o wystarczających gwarancjach odnośnie do technicznych środków bezpieczeństwa oraz rozwiązań organizacyjnych, regulujących przetwarzanie danych, oraz do zapewnienia stosowania tych środków i rozwiązań[54]; - administrator danych poleca przetwarzającemu, pośrednikowi, wykonawcy lub innemu dostawcy usług zapewnianie w szczególności, aby: <ul style="list-style-type: none"> (i) działali oni wyłącznie na polecenie administratora danych[55]; (ii) zasady dotyczące bezpieczeństwa i poufności były obowiązkowe dla przetwarzającego, pośrednika, wykonawcy lub innego dostawcy usług[56]. <p>Administrator danych może wydawać</p>

<p>umownych zgodnie z art. 25 i 26 dyrektywy UE)[52];</p> <ul style="list-style-type: none"> - wszelkie przypadki przekazywania danych zewnętrznym przetwarzającym z siedzibą poza UE były zgodne nie tylko z przepisami dotyczącymi transgranicznego przepływu danych (art. 25–26 dyrektywy 95/46/WE), ale również z przepisami dotyczącymi przetwarzających (art. 16–17 dyrektywy 95/45/WE)[53]. 	<p>polecenia[57]:</p> <ul style="list-style-type: none"> - za pośrednictwem wewnętrznych wytycznych lub polityk; lub - za pośrednictwem umów; lub - zapewniając zgodność z przepisami ustawowymi i wykonawczymi dotyczącymi danej branży przemysłowej lub sektora; lub - stosując kodeks lub zasady organu samoregulacyjnego; lub - za pośrednictwem innych środków. <p>Zgodnie z wspomnianymi uzgodnieniami zasadniczo wymaga się, aby przetwarzający, pośrednicy, wykonawcy lub inni dostawcy usług wykorzystujący dane osobowe stosowali odpowiednie środki ochrony spośród następujących możliwości[58]:</p> <ul style="list-style-type: none"> - przestrzeganie polityk i praktyk ochrony prywatności zgodnych z normami APEC, stosowanych przez administratora danych, określonych w oświadczeniu administratora danych o polityce ochrony prywatności; - wdrażanie praktyk ochrony prywatności, które są zasadniczo podobne do polityki i praktyk ochrony prywatności stosowanych przez administratora danych, określonych w oświadczeniu administratora danych o polityce ochrony prywatności; - wykonywanie poleceń wydawanych przez administratora danych, dotyczących sposobu obchodzenia się z danymi osobowymi administratora danych; - nakładanie ograniczeń na podwykonawstwo, chyba że zleca się je za zgodą administratora danych; - uzyskanie certyfikacji CBPR przeprowadzanej przez pełnomocnika APEC odpowiedzialnego za rozliczalność
---	---

	<p>w ich jurysdykcji;</p> <p>- inne środki.</p> <p>Przetwarzający, pośrednicy, wykonawcy lub inni dostawcy usług powiadają administratora danych o przypadkach naruszenia prywatności lub bezpieczeństwa danych osobowych administratora danych w przypadku gdy dowiedzą się o takim naruszeniu[59].</p> <p>Przetwarzający, pośrednicy, wykonawcy lub inni dostawcy usług natychmiast podejmują działania w celu naprawienia/wyeliminowania niedopatrzeń w zakresie bezpieczeństwa, które spowodowały naruszenie prywatności lub bezpieczeństwa[60].</p> <p>Przetwarzający, pośrednicy, wykonawcy lub inni dostawcy usług przedstawiają administratorowi danych samooceny w celu zapewnienia zgodności z poleceniami administratora danych lub uzgodnieniami/umowami[61].</p> <p>Administrator danych przeprowadza regularne kontrole wrywkowe lub monitoruje przetwarzających, pośredników, wykonawców lub innych dostawców usług wykorzystujących jego dane osobowe w celu zapewnienia zgodności z jego poleceniami lub uzgodnieniami/umowami[62].</p>
--	--

Dokumenty odniesienia

[50] UE: zob. WP74, pkt 3.2, s. 9–10; APEC: zob. kwestionariusz wstępny, pyt. 47, s. 22.

[51] UE: zob. dyrektywa 95/46, art. 17 ust. 2; WP154, pkt 12, s. 7.

[52] UE: zob. WP74, pkt 3.2, s. 9–10.

[53] UE: zob. WP154, pkt 12, s. 7.

[54] APEC: zob. kwestionariusz wstępny, pyt. 35, s. 15.

[55] APEC: zob. kwestionariusz wstępny, pyt. 47–48, s. 22–23.

[56] APEC: zob. kwestionariusz wstępny, pyt. 35, s. 15–16.

[57] APEC: zob. kwestionariusz wstępny, pyt. 46, s. 22.

[58] APEC: zob. kwestionariusz wstępny, pyt. 47, s. 22–23.

[59] APEC: zob. kwestionariusz wstępny, pyt. 35 lit. b), s. 15.

[60] APEC: zob. kwestionariusz wstępny, pyt. 35 lit. c), s. 16.

[61] APEC: zob. kwestionariusz wstępny, pyt. 48, s. 23.

[62] APEC: zob. kwestionariusz wstępny, pyt. 49, s. 23.

9. Definicje

Elementy wspólne wymagane zarówno do zatwierdzenia BCR, jak i certyfikacji CBPR

Oczekuje się, że organizacja będzie interpretowała terminy zawarte w swoich zasadach ochrony danych osobowych i prywatności zgodnie z obowiązującymi przepisami UE, w szczególności zgodnie z dyrektywą 95/46/WE i dyrektywą 2002/58/WE, przepisami mającymi zastosowanie w gospodarkach uczestniczących w CBPR oraz zgodnie z glosariuszem APEC dotyczącym systemu CBPR[63].

Elementy dodatkowe wymagane do zatwierdzenia BCR	Elementy dodatkowe wymagane do certyfikacji CBPR
Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą zawierać zobowiązanie do interpretowania terminów zgodnie z mającymi zastosowanie przepisami UE, w szczególności zgodnie z dyrektywą 95/46/WE i dyrektywą 2002/58/WE, oraz muszą zawierać opis następujących głównych terminów i ich definicje: dane osobowe[64]; administrator danych[65]; przetwarzający[66]; osoby, których dane dotyczą[67]; dane osobowe szczególnie chronione[68]; przetwarzanie danych osobowych[69]; osoba trzecia[70]; oraz organy ochrony danych UE[71].	Nie dotyczy

Dokumenty odniesienia

[63] UE: zob. WP154, pkt 2, s. 4; WP155 pyt. 8, s. 5; APEC: zob. glosariusz dotyczący systemu CBPR.

[64] UE: zob. dyrektywa 95/46, art. 2 lit. a).

[65] UE: zob. dyrektywa 95/46, art. 2 lit. d).

[66] UE: zob. dyrektywa 95/46, art. 2 lit. e).

[67] UE: zob. dyrektywa 95/46, art. 2 lit. a).

[68] UE: zob. dyrektywa 95/46, art. 8.

[69] UE: zob. dyrektywa 95/46, art. 2 lit. b).

[70] UE: zob. dyrektywa 95/46, art. 2 lit. f).

[71] UE: zob. dyrektywa 95/46, art. 2 lit. f).

10. Gromadzenie, przetwarzanie i wykorzystywanie danych osobowych

Elementy wspólne wymagane zarówno do zatwierdzenia BCR, jak i certyfikacji CBPR

Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą stanowić, że dane osobowe są gromadzone i przetwarzane wyłącznie w sposób rzetelny i legalny^[72] do określonych celów i nie można ich wykorzystywać w sposób niezgodny z tymi celami, zgodnie z definicją tego terminu określoną w obowiązujących przepisach^[73].

Elementy dodatkowe wymagane do zatwierdzenia BCR Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą również stanowić, że dane osobowe będą przekazywane i przetwarzane wyłącznie do celów jednoznacznych i uzasadnionych ^[74] .	Elementy dodatkowe wymagane do certyfikacji CBPR Nie dotyczy
Wyjaśnienie przetwarzania danych osobowych (BCR) Nie dotyczy	Wyjaśnienie wykorzystywania danych osobowych (CBPR) Dane osobowe można wykorzystywać do innych zgodnych i powiązanych celów za zgodą osoby, której dane osobowe są gromadzone; w razie potrzeby w celu świadczenia usługi lub dostarczenia produktu, których życzy sobie dana osoba, lub z mocy prawa i innych instrumentów prawnych, proklamacji i oświadczeń dotyczących skutków prawnych ^[75] .

Dokumenty odniesienia

[72] UE: zob. dyrektywa 95/46, art. 6 ust. 1 lit. a); WP108, pkt 8.2.1, s. 8; WP153, pkt 6.1 ppkt (i), s. 10; WP154, pkt 5, s. 4, pkt 6, s. 5; APEC: zob. ramowe zasady prywatności, część (iii), zasada III, pkt 18, s. 15; wymogi programowe, pyt. 7, s. 7.

[73] UE: zob. dyrektywa 95/46, art. 6 ust. 1 lit. b); WP108, pkt 8.2.2, s. 8; WP153, pkt 6.1 ppkt (ii), s. 10; WP154, pkt 3, s. 4; APEC: zob. ramowe zasady prywatności, część (iii), zasady III i IV, pkt 18 i 19, s. 15–16; wymogi programowe, pyt. 6 i 8, s. 6 i 8.

[74] UE: zob. dyrektywa 95/46, art. 6 ust. 1 lit. b); WP108, pkt 8.2.2, s. 8; WP153, pkt 6.1 ppkt (ii), s. 10; WP154, pkt 3, s. 4.

[75] APEC: zob. ramowe zasady prywatności, część (iii), zasada IV, pkt 19, s. 16–17; wymogi programowe pyt. 9 i 13, s. 8–10.

11. Jakość i proporcjonalność danych/integralność danych

Elementy wspólne wymagane zarówno do zatwierdzenia BCR, jak i certyfikacji CBPR

Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą zawierać zobowiązanie, zgodnie z którym:

- dane osobowe muszą być dokładne, kompletne i w stosownych przypadkach aktualizowane. Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą również zawierać zobowiązanie do powiadamiania, w stosownych przypadkach, wszystkich właściwych stron o wspomnianych korektach[76];
- dane osobowe muszą być prawidłowe i odpowiednie w stosunku do celów, dla których są one przekazywane lub dalej przetwarzane[77].

Elementy dodatkowe wymagane do zatwierdzenia BCR	Elementy dodatkowe wymagane do certyfikacji CBPR
<p>Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą również zawierać wyraźny wymóg, zgodnie z którym dane osobowe nie mogą być nadmierne ilościowo w stosunku do celów, dla których są one przekazywane i dalej przetwarzane[78].</p> <p>Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą również zawierać wymóg, zgodnie z którym dane osobowe mogą być przetwarzane przez czas nie dłuższy niż jest to konieczne do celów, dla których dane zostały zgromadzone lub, w razie potrzeby, dla których są dalej przetwarzane[79].</p>	<p>Nie dotyczy</p>

Dokumenty odniesienia

[76] UE: zob. dyrektywa 95/46, art. 6 ust. 1 lit. d); WP153, pkt 6.1 ppkt (iii), s. 10; WP108, pkt 8.2.3, s. 8; APEC: zob. ramowe zasady prywatności, część (iii), zasada IV, pkt 21, s. 20; wymogi programowe pkt 21, 22, s. 15; kwestionariusz wstępny, pyt. 22, 23 i 24, s. 13.

[77] UE: zob. dyrektywa 95/46, art. 6 ust. 1 lit. c); WP153, pkt 6.1 ppkt (iii), s. 10; WP108, pkt 8.2.3, s. 8; APEC: zob. ramowe zasady prywatności, część (iii), zasada III, pkt 18, s. 15; wymogi programowe, pyt. 6, s. 6.

[78] UE: zob. dyrektywa 95/46, art. 6 ust. 1 lit. d); WP153, pkt 6.1 ppkt (iii), s. 10.

[79] UE: zob. dyrektywa 95/46, art. 6 ust. 1 lit. e); WP153, pkt 6.1 ppkt (iii), s. 10; WP108, pkt 8.2.3, s. 8.

12. Podstawy przetwarzania danych osobowych

Elementy wspólne wymagane zarówno do zatwierdzenia BCR, jak i certyfikacji CBPR

Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą zawierać zobowiązanie, zgodnie z którym:

- dane osobowe są przetwarzane (w tym gromadzone, wykorzystywane, przekazywane, ujawniane lub udostępniane) wyłącznie w przypadku, gdy istnieją uzasadnione podstawy do przetwarzania, takie jak świadoma zgoda osoby fizycznej/osoby, których dane dotyczą[80];
- dane osobowe są przetwarzane zgodnie z prawem mającym zastosowanie[81].

Elementy dodatkowe wymagane do zatwierdzenia BCR	Elementy dodatkowe wymagane do certyfikacji CBPR
<p>Jeżeli zgoda stanowi podstawę prawną do przetwarzania, powinna ona być jednoznaczna, szczegółowa, udzielona z własnej woli i świadoma[82].</p> <p>Nie można wykluczyć zgody jako podstawy prawnej do przetwarzania danych ze względu na oczywistość, publiczną dostępność danych osobowych, fakt, iż udzielenie zgody jest niewykonalne w praktyce ze względów technologicznych ani z powodu otrzymania danych osobowych od osoby trzeciej.</p> <p>Zgoda stanowi tylko jedną z możliwych podstaw prawnych do przetwarzania danych osobowych.</p> <p>Dane osobowe można również przetwarzać w oparciu o następujące podstawy[83]:</p> <ul style="list-style-type: none">- przetwarzanie danych jest konieczne dla realizacji umowy, której stroną jest osoba, której dane dotyczą, lub w celu podjęcia działań na życzenie osoby, której dane dotyczą, przed zawarciem umowy; lub- przetwarzanie danych jest konieczne dla wykonania zobowiązania prawnego UE, któremu administrator danych podlega;- przetwarzanie danych jest konieczne dla zapewnienia ochrony żywotnych	<p>Nie dotyczy</p>

<p>interesów osoby, której dane dotyczą; lub</p> <ul style="list-style-type: none"> - przetwarzanie danych jest konieczne dla realizacji zadania wykonywanego w interesie publicznym lub dla wykonywania władzy publicznej UE powierzonej administratorowi danych lub osobie trzeciej, której ujawnia się dane; lub - przetwarzanie danych jest konieczne dla potrzeb wynikających z uzasadnionych interesów administratora danych lub osoby trzeciej, lub osób, którym dane są ujawniane, z wyjątkiem sytuacji, kiedy interesy takie podporządkowane są interesom związanym z podstawowymi prawami i wolnościami osoby, której dane dotyczą. 	
<p>Wyjaśnienie powodów przetwarzania (BCR)</p> <p>Nie dotyczy</p>	<p>Wyjaśnienie powodów przetwarzania (CBPR)</p> <p>Osoby fizyczne powinny móc wybrać, czy zgadzają się na gromadzenie, wykorzystywanie i ujawnianie ich danych osobowych. Zgodnie z tą zasadą uznaje się jednak, przez wyrażenie wprowadzające „w stosownych przypadkach” w samych ramowych zasadach prywatności, że istnieją określone sytuacje, w których zgoda może być wyraźnie dorozumiana lub w których nie jest konieczne zapewnienie mechanizmu wyboru. Sytuacje te są szczegółowo opisane w „Zastrzeżeniach dotyczących zapewniania mechanizmów wyboru”[84].</p> <p>Zgodnie z wymienionymi zastrzeżeniami osobom fizycznym należy zapewnić:</p> <ul style="list-style-type: none"> - zrozumiały i przejrzysty mechanizm wyboru w związku z gromadzeniem ich danych osobowych; - zrozumiały i przejrzysty mechanizm wyboru w związku z wykorzystywaniem ich danych

	<p>osobowych;</p> <ul style="list-style-type: none"> - zrozumiały i przejrzysty mechanizm wyboru w związku z ujawnianiem ich danych osobowych; - mechanizmy te muszą być jasno sformułowane, łatwe do zrozumienia, łatwo dostępne i przystępne. <p>Zastrzeżenia mające zastosowanie obejmują:</p> <ul style="list-style-type: none"> - oczywistość; - gromadzenie publicznie dostępnych informacji; - niewykonalność w praktyce ze względów technologicznych; - przyjęcie danych od osoby trzeciej; - ujawnienie danych instytucji rządowej, która wnioskuje o dane informacje na podstawie upoważnienia z mocy prawa; - ujawnienie danych osobie trzeciej na podstawie zgodnej z prawem formy przetwarzania; - cele związane z uzasadnionym dochodzeniem; - działanie na wypadek sytuacji wyjątkowej. <p>Poza przetwarzaniem danych osobowych za zgodą można je również przetwarzać w oparciu o następujące podstawy[85]:</p> <ul style="list-style-type: none"> - do zgodnych lub powiązanych celów, określonych w oświadczeniu o polityce ochrony prywatności lub piśmie przedstawionym w czasie gromadzenia danych; - w przypadku, gdy dane są niezbędne do świadczenia usługi lub dostarczenia produktu, których życzy sobie osoba fizyczna; - w przypadku gdy dane są wymagane
--	---

	zgodnie z obowiązującymi przepisami.
--	--------------------------------------

Dokumenty odniesienia

- [80] UE: zob. dyrektywa 95/46, art. 7 lit. a); WP154, pkt 5, s. 4; APEC: zob. ramowe zasady prywatności, część (iii), zasada III, pkt 18, s. 15.
- [81] UE: zob. WP153, pkt 6.4, s. 11; WP155 pyt. 10, s. 6; APEC: zob. wymogi programowe, pyt. 7, s. 7.
- [82] UE: zob. dyrektywa 95/46, art. 7 lit. a); WP154, pkt 5, s. 4.
- [83] UE: zob. dyrektywa 95/46, art. 7; WP154, pkt 5, s. 4.
- [84] APEC: zob. wymogi programowe, pyt. 14, 15, 16, 17, 18, 19, s. 11–14.
- [85] APEC: zob. wymogi programowe, pyt. 8, 9, 10, 11, 12, 13, s. 8–10.

13. Dane sensytywne

Elementy wspólne wymagane zarówno do zatwierdzenia BCR, jak i certyfikacji CBPR

W zasadach organizacji dotyczących ochrony danych osobowych i prywatności należy wskazać odpowiednie sposoby ochrony mające zastosowanie do danych sensytywnych[86].

Elementy dodatkowe wymagane do zatwierdzenia BCR	Elementy dodatkowe wymagane do certyfikacji CBPR
<p>Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą również zawierać zobowiązanie, zgodnie z którym przetwarzanie danych sensytywnych (np. danych osobowych ujawniających pochodzenie rasowe lub etniczne; opinie polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych oraz danych dotyczących życia seksualnego i zdrowia) są zabronione z wyjątkiem sytuacji, w których[87]:</p> <ul style="list-style-type: none">- osoba, której dane dotyczą, udzieliła wyrażnej zgody na przetwarzanie tych danych sensytywnych, z wyjątkiem przypadków, w których zakazują tego obowiązujące przepisy; lub- przetwarzanie danych jest konieczne do wypełniania obowiązków i szczególnych uprawnień administratora danych w dziedzinie prawa pracy UE, o ile jest to dozwolone przez prawo krajowe przewidujące odpowiednie środki zabezpieczające; lub- przetwarzanie danych jest konieczne dla ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, w przypadku gdy osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do udzielenia zgody; lub- przetwarzanie danych jest dokonywane w ramach legalnej działalności wspartej odpowiednimi gwarancjami przez fundację, stowarzyszenie lub inną instytucję nienastawioną na osiągnięcie	<p>Przy określaniu dozwolonych sposobów wykorzystywania informacji należy wziąć pod uwagę charakter danych informacji[89].</p> <p>Wdrażane środki zabezpieczające muszą być uzasadnione i proporcjonalne do prawdopodobieństwa wystąpienia i wagi zagrażającej szkody, wrażliwości danych i kontekstu, w którym są one przechowywane[90].</p>

<p>zysku, której cele mają charakter polityczny, filozoficzny, religijny lub związkowy, pod warunkiem że przetwarzanie danych odnosi się wyłącznie do członków tej instytucji lub osób mających z nią regularny kontakt w związku z jej celami oraz, że dane nie zostaną ujawnione osobie trzeciej bez zgody osób, których dane dotyczą; lub</p> <ul style="list-style-type: none"> - przetwarzanie dotyczy danych sensytywnych, które są wyraźnie podawane do wiadomości publicznej przez osobę, której dane dotyczą; lub - przetwarzanie danych sensytywnych jest konieczne do ustalenia, wykonania lub ochrony roszczeń prawnych; lub - przetwarzanie danych sensytywnych wymagane jest do celów medycyny prewencyjnej, diagnostyki medycznej, świadczenia opieki lub leczenia, lub też zarządzania opieką zdrowotną, jak również w przypadkach, gdy dane szczególnie chronione są przetwarzane przez pracownika służby zdrowia zgodnie z przepisami prawa krajowego lub zasadami określonymi przez właściwe krajowe instytucje, podlegającemu obowiązkowi zachowania tajemnicy zawodowej lub przez inną osobę również zobowiązaną do zachowania tajemnicy. <p>Dane sensytywne należy przetwarzać, stosując wzmocnione środki bezpieczeństwa[88].</p>	
---	--

Dokumenty odniesienia

[86] UE: zob. dyrektywa 95/46, art. 8; WP154, pkt 6, s. 5; APEC: zob. ramowe zasady prywatności, część (iii), zasada VII, pkt 22, s. 21.

[87] UE: zob. dyrektywa 95/46, art. 8; WP154, pkt 6, s. 5.

[88] UE: zob. dyrektywa 95/46, art. 17 ust. 1; WP154, pkt 10, s. 7.

[89] APEC: zob. wymogi programowe, s. 8.

[90] APEC: zob. ramowe zasady prywatności, część (iii), zasada VII, pkt 22, s. 21; wymogi programowe pyt. 28, 30, 35 lit. a), s. 18–20.

14. Przejrzystość i prawo do informacji/powiadomienia

Elementy wspólne wymagane zarówno do zatwierdzenia BCR, jak i certyfikacji CBPR

Organizacja musi udostępniać oświadczenie o polityce ochrony prywatności każdej osobie, której dane dotyczą, przed lub w trakcie gromadzenia danych[91]. W oświadczeniu tym musi znajdować się opis:

- sposobu informowania osób, których dane dotyczą, o przekazaniu i przetwarzaniu ich danych osobowych[92];
- tożsamości administratora lub administratorów danych i ewentualnie jego przedstawicieli oraz punktów kontaktowych[93];
- przewidzianych celów przetwarzania zgromadzonych danych[94];
- wszelkich dalszych informacji, jak np.:
 - (i) odbiorcy lub kategorie odbierających danych[95];
 - (ii) istnienie prawa dostępu do swoich danych oraz ich sprostowania, jak również sposób, w jaki osoby, których dane dotyczą, mogą uzyskać dostęp do swoich danych osobowych[96].

W przypadku gdy źródłem uzyskiwania danych nie jest osoba, której dane dotyczą, zachodzą okoliczności, w których obowiązek informowania osoby, której dane dotyczą, może nie mieć zastosowania[97]. Wyjątki takie różnią się w przypadku BCR i w przypadku CBPR. Wymogi dla poszczególnych programów w odniesieniu do BCR i w odniesieniu do CBPR należy określić w zasadach ochrony danych osobowych i prywatności danej organizacji.

Elementy dodatkowe wymagane do zatwierdzenia BCR	Elementy dodatkowe wymagane do certyfikacji CBPR
<p>Dalsze informacje należy przedstawić osobom, których dane dotyczą, o ile informacje takie są potrzebne, biorąc pod uwagę szczególne okoliczności, w których dane są gromadzone, w celu zagwarantowania rzetelnego przetwarzania danych w stosunku do osoby, której dane dotyczą[98].</p> <p>W przypadku gdy dane uzyskiwane są z innych źródeł niż osoba, której dane dotyczą, obowiązek informowania osoby, której dane dotyczą, nie ma zastosowania, jeżeli dostarczenie takich informacji okazałoby się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku lub jeżeli gromadzenie lub ujawnianie informacji jest wyraźnie przewidziane przez prawo[99].</p> <p>Chociaż obowiązek informowania osoby, której dane dotyczą, może nie mieć</p>	<p>Organizacja musi również poinformować osoby, których dane dotyczą, o sposobie gromadzenia danych i o tym, czy są one gromadzone[100]:</p> <ul style="list-style-type: none">- bezpośrednio od osób fizycznych; lub- od osób trzecich gromadzących dane w imieniu administratora danych; lub- z innych źródeł (należy je opisać). <p>Istnieją okoliczności, w których powiadomienie może nie być konieczne lub może być niepraktyczne[101]:</p> <ul style="list-style-type: none">- oczywistość;- gromadzenie publicznie dostępnych informacji;- niewykonalność w praktyce z

<p>zastosowania we wspomnianych powyżej okolicznościach, nie można go wykluczyć ze względu na oczywistość, publiczną dostępność danych osobowych, fakt, iż poinformowanie osoby, której dane dotyczą, jest niewykonalne w praktyce ze względów technologicznych ani z powodu otrzymania danych osobowych od osoby trzeciej.</p>	<p>powodów technologicznych;</p> <ul style="list-style-type: none"> - ujawnienie danych instytucji rządowej, która wnioskuje o dane informacje na podstawie upoważnienia z mocy prawa; - ujawnienie danych osobie trzeciej na podstawie zgodnej z prawem formy przetwarzania; - przyjęcie danych od osoby trzeciej; - cele związane z uzasadnionym dochodzeniem; - działanie na wypadek sytuacji wyjątkowej. <p>Dodatkowe informacje, które należy przedstawić osobom, których dane dotyczą:</p> <ul style="list-style-type: none"> - fakt gromadzenia danych osobowych^[102]; - cel, w jakim dane udostępnia się osobom trzecim^[103]; - informacje dotyczące wykorzystywania i ujawniania danych osób, których dane dotyczą^[104]; - wybór i środki oferowane osobom, których dane dotyczą, w celu ograniczenia wykorzystywania i ujawniania ich danych osobowych^[105].
---	---

Dokumenty odniesienia

[91] UE: zob. dyrektywa 95/46, art. 10 i 11; WP153, pkt 1.7, s. 5; WP74, pkt 5.7, s. 19, WP154, pkt 7, s. 5; APEC: zob. ramowe zasady prywatności, część (iii), zasada II, pkt 15 i 16, s. 12–13 oraz pkt 16 s. 13.

[92] UE: zob. WP74, pkt 5.7, s. 19; WP153, pkt 6.1 ppkt (i), s. 10; APEC: zob. kwestionariusz wstępny, pyt. 1, s. 4; pyt. 17–19, s. 10–11.

[93] UE: zob. WP154, pkt 7, s. 5; APEC: zob. kwestionariusz wstępny, pyt. 1 lit. d), s. 4–5.

[94] UE: zob. WP154, pkt 7, s. 5; APEC: zob. kwestionariusz wstępny, pyt. 1 lit. b) i pyt. 3, s. 4–5.

[95] UE: zob. WP154, pkt 7, s. 5; APEC: zob. ramowe zasady prywatności, część (iii), zasada II, pkt 15 lit. c), s. 12.

[96] UE: zob. WP154, pkt 7, s. 5; APEC: zob. ramowe zasady prywatności, część (iii), zasada II, pkt 15

- lit. e), s. 12; kwestionariusz wstępny, pyt. 38 lit. a), s. 18.
- [97] UE: zob. dyrektywa 95/46, art. 10 i 11; APEC: zob. kwestionariusz wstępny, zastrzeżenia dotyczące dostarczenia powiadomienia, s. 6.
- [98] UE: zob. dyrektywa 95/46, art. 10.
- [99] UE: zob. dyrektywa 95/46, art. 11.
- [100] APEC: zob. kwestionariusz wstępny, pyt. 1 lit. a), s. 4 i pyt. 5, s. 7.
- [101] APEC: zob. kwestionariusz wstępny, zastrzeżenia dotyczące dostarczenia powiadomienia, s. 6.
- [102] APEC: zob. ramowe zasady prywatności, część (iii), zasada II, pkt 15 lit. a), s. 12.
- [103] APEC: zob. kwestionariusz wstępny, pyt. 1 lit. c), s. 4.
- [104] APEC: zob. kwestionariusz wstępny, pyt. 1 lit. e), s. 5.
- [105] APEC: zob. ramowe zasady prywatności, część (iii), zasada II, pkt 15 lit. e), s. 12; kwestionariusz wstępny, pyt. 15–16, s. 10.

15. Prawo dostępu, prawo do sprostowania, usunięcia lub zablokowania danych/dostępu do danych i prawo do korekty danych

Elementy wspólne wymagane zarówno do zatwierdzenia BCR, jak i certyfikacji CBPR

Organizacja musi zapewnić, aby^[106]:

- każda osoba, której dane dotyczą, była w stanie uzyskać od administratora danych potwierdzenie, czy posiada on dotyczące jej dane osobowe^[107];
- każda osoba, której dane dotyczą, była w stanie uzyskać kopię wszystkich dotyczących jej danych posiadanych przez organizację. Należy dostarczyć odpowiednie dane bez ograniczeń, w rozsądnym terminie i za niezawyżoną opłatą (o ile dotyczy)^[108];
- każda osoba, której dane dotyczą, mogła wymagać od administratora danych sprostowania lub usunięcia danych, które są w sposób szczególny niekompletne lub nieprawidłowe^[109].

Zobowiązania te podlegają wyłączeniom i zastrzeżeniom zgodnie z obowiązującymi przepisami^[110].

Elementy dodatkowe wymagane do zatwierdzenia BCR	Elementy dodatkowe wymagane do certyfikacji CBPR
<p>Elementami wymienionymi w powyższej wspólnej liście kontrolnej są prawa przyznane osobom, których dane dotyczą.</p> <p>Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą również zapewniać, aby każdej osobie, której dane dotyczą, przysługiwało prawo wymagania od administratora danych zablokowania danych, w szczególności w przypadkach, w których dane są niekompletne lub nieprawidłowe^[111].</p>	<p>Administratorzy danych muszą podjąć działania mające na celu potwierdzenie tożsamości osoby, której dane dotyczą, zwracającej się o dostęp do danych^[112].</p> <p>Jeżeli informacje przedstawia się osobie, której dane dotyczą i która skorzystała z prawa dostępu, należy je przekazać w sposób rozsądny, powszechnie zrozumiały i zgodny ze standardową formą komunikowania się z daną osobą fizyczną^[113].</p> <p>Zobowiązanie do dokonania korekt lub usunięcia w rozsądnym terminie^[114].</p> <p>Administratorzy danych muszą przedstawić osobie, której dane dotyczą, kopię poprawionych danych osobowych lub potwierdzenie korekty bądź usunięcia jej danych osobowych^[115].</p> <p>Administratorzy danych muszą przedstawić osobom, których dane dotyczą, wyjaśnienie, dlaczego nie zapewnia się im dostępu do danych lub możliwości skorygowania danych oraz informacje kontaktowe na wypadek dalszych pytań dotyczących odmowy dostępu</p>

	lub korekty ^[116] .
<p>Wyjątki od prawa dostępu (BCR)</p> <p>W krajowych przepisach UE o ochronie danych mogą być przewidziane pewne wyjątki od prawa dostępu przysługującego osobom, których dane dotyczą, na podstawie prawa krajowego UE i które powinny podlegać wykładni zawężającej; w takich przypadkach może być konieczne, aby organizacje odrzuciły wnioski o dostęp w celu zabezpieczenia w państwach członkowskich UE^[117]:</p> <ul style="list-style-type: none"> a) bezpieczeństwa narodowego; b) obronności; c) bezpieczeństwa publicznego; d) działań prewencyjnych, prowadzonych czynności dochodzeniowo-śledczych i prokuratorskich w sprawach karnych lub sprawach o naruszenie zasad etyki w zawodach podlegających regulacji; e) ważnego interesu ekonomicznego lub finansowego państwa członkowskiego lub Unii Europejskiej, łącznie z kwestiami pieniężnymi, budżetowymi i podatkowymi; f) funkcji kontrolnych, inspekcyjnych i regulacyjnych związanych, nawet sporadycznie, z wykonywaniem władzy publicznej w przypadkach wymienionych w lit. c), d) i e); g) ochrony osoby, której dane dotyczą, lub praw i wolności innych osób. <p>Przepisy UE o ochronie danych krajowych mogą przewidywać, z zastrzeżeniem obowiązku zapewnienia odpowiedniego stopnia ochrony prawnej, w szczególności, aby dane nie były wykorzystywane do podejmowania działań lub decyzji dotyczących jakichkolwiek konkretnych osób, że prawo dostępu przysługujące osobom,</p>	<p>Wyjątki od prawa dostępu (CBPR)</p> <p>Istnieją okoliczności, w których konieczne może być, aby organizacje odrzucały wnioski o udzielenie dostępu^[118]:</p> <ul style="list-style-type: none"> - nieproporcjonalne obciążenie; - ochrona informacji poufnych; - ryzyko osoby trzeciej.

<p>których dane dotyczą, może, w przypadku gdy wyraźnie nie występuje ryzyko naruszenia prywatności osoby, której dane dotyczą, być ograniczone, gdy dane są przetwarzane wyłącznie do celów badań naukowych lub przechowywane w formie osobistej przez okres nieprzekraczający okresu koniecznego wyłącznie w celu sporządzenia statystyk.</p>	
---	--

Dokumenty odniesienia

- [106] UE: zob. dyrektywa 95/46, art. 12; WP153, pkt 6.1 ppkt (v), s. 10; WP108, pkt 8.2.5, s. 8.
- [107] APEC: zob. ramowe zasady prywatności, część (iii), zasada VIII, pkt 23 lit. a), s. 22; kwestionariusz wstępny, pyt. 36, s. 17.
- [108] APEC: zob. ramowe zasady prywatności, część (iii), zasada VIII, pkt 23 lit. b), s. 22; kwestionariusz wstępny, pyt. 37, pyt. 37 lit. b) i pyt. 37 lit. c), s. 17–18.
- [109] APEC: zob. ramowe zasady prywatności, część (iii), zasada VIII, pkt 23 lit. c), s. 22; kwestionariusz wstępny, pyt. 38, pyt. 38 lit. b), s. 18–19.
- [110] UE: zob. dyrektywa 95/46, art. 13; APEC: zob. kwestionariusz wstępny, zastrzeżenia dotyczące zapewniania dostępu i mechanizmów poprawy danych, s. 19–20.
- [111] UE: zob. dyrektywa 95/46, art. 12.
- [112] APEC: zob. kwestionariusz wstępny, pyt. 37 lit. a), s. 17.
- [113] APEC: zob. kwestionariusz wstępny, pyt. 37 lit. c) i d), s. 18.
- [114] APEC: zob. kwestionariusz wstępny, pyt. 38 lit. a), s. 19.
- [115] APEC: zob. kwestionariusz wstępny, pyt. 38 lit. d), s. 19.
- [116] APEC: zob. ramowe zasady prywatności, część (iii), zasada VIII, pkt 25, s. 24; kwestionariusz wstępny, pyt. 38 lit. e), s. 19.
- [117] UE: zob. dyrektywa 95/46, art. 13.
- [118] APEC: zob. kwestionariusz wstępny, zastrzeżenia dotyczące zapewnienia dostępu i mechanizmów poprawy danych, s. 19–20.

16. Prawo sprzeciwu/wybór

Elementy wspólne wymagane zarówno do zatwierdzenia BCR, jak i certyfikacji CBPR

W stosownych przypadkach lub jeżeli jest to wymagane na podstawie obowiązujących przepisów organizacja musi zapewnić, aby osoba, której dane dotyczą, mogła nie zgodzić się na przetwarzanie jej danych osobowych lub mieć wybór dotyczący tego, czy chce, aby jej dane osobowe były objęte przetwarzaniem, zgodnie z obowiązującymi przepisami[119].

Elementy dodatkowe wymagane do zatwierdzenia BCR	Elementy dodatkowe wymagane do certyfikacji CBPR
<p>Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą również zapewniać, aby każda osoba, której dane dotyczą, miała prawo sprzeciwu wobec przetwarzania jej danych osobowych, ponieważ jest to prawo przyznane osobom, których dane dotyczą.</p> <p>Osoba, której dane dotyczą, może skorzystać z prawa sprzeciwu w każdej chwili.</p> <p>W szczególności każda osoba, której dane dotyczą, ma prawo sprzeciwu, na wniosek i bez opłaty, wobec przetwarzania dotyczących jej danych osobowych, które zdaniem administratora danych są przetwarzane dla potrzeb bezpośredniego obrotu, lub prawo bycia poinformowanym przed ujawnieniem danych osobowych po raz pierwszy osobom trzecim lub ich wykorzystaniem w ich imieniu dla potrzeb bezpośredniego obrotu, jak również prawo wyraźnego powoływania się na prawo sprzeciwu, bez opłat, wobec ujawniania lub wykorzystywania danych.</p>	<p>Nie dotyczy</p>
<p>Wyjątki od prawa sprzeciwu (BCR)</p> <p>Nie dotyczy</p>	<p>Wyjątki dotyczące wyboru (CBPR)</p> <p>Istnieją okoliczności, w których zapewnienie osobom fizycznym mechanizmów wyboru może nie być konieczne lub może być niepraktyczne dla organizacji[120]:</p> <ul style="list-style-type: none">- oczywistość;- gromadzenie publicznie dostępnych informacji;

	<ul style="list-style-type: none"> - niewykonalność w praktyce ze względów technologicznych; - przyjęcie danych od osoby trzeciej; - ujawnienie danych instytucji rządowej, która wnioskuje o dane informacje na podstawie upoważnienia z mocy prawa; - ujawnienie danych osobie trzeciej na podstawie zgodnej z prawem formy przetwarzania; - cele związane z uzasadnionym dochodzeniem; - działanie na wypadek sytuacji wyjątkowej.
<p>Wyjaśnienie prawa sprzeciwu (BCR)</p> <p>Osobie, której dane dotyczą, zawsze przysługuje prawo wycofania swojej zgody. Ponadto w przypadkach, w których istnieje dodatkowa podstawa prawna uzasadniająca przetwarzanie danych, osoba, której dane dotyczą, nadal może wnieść swój sprzeciw.</p> <p>Co więcej, w przepisach UE o ochronie danych krajowych przewiduje się okoliczności, w których osoby, których dane dotyczą, mogą, przynajmniej w przypadkach, gdy podstawa prawna dla przetwarzania danych wynika z art. 7 lit. e) lub f) dyrektywy 95/46/WE, sprzeciwić się z ważnych i uzasadnionych przyczyn związanych z ich szczególną sytuacją, chyba że przepisy krajowe państw członkowskich UE stanowią inaczej. W przypadku uzasadnionego sprzeciwu przetwarzanie danych przez administratora danych nie może już obejmować tych danych^[121].</p> <p>Nie można wykluczyć prawa sprzeciwu ze względu na oczywistość, publiczną dostępność przetwarzanych danych osobowych, niewykonalność prawa sprzeciwu w praktyce ze względów technologicznych</p>	<p>Wyjaśnienie wyboru (CBPR)</p> <p>Organizacje są zobowiązane do zapewnienia osobom fizycznym mechanizmów wyboru w odniesieniu do gromadzenia, wykorzystywania i ujawniania ich danych osobowych^[122].</p>

ani ze względu na otrzymanie danych osobowych od osoby trzeciej.	
--	--

Dokumenty odniesienia

[119] UE: zob. dyrektywa 95/46, art. 14; WP153, pkt 6.1 ppkt (v), s. 10; WP108, pkt 8.2.5, s. 8; APEC: zob. kwestionariusz wstępny, pyt 14–16.

[120] APEC: zob. kwestionariusz wstępny, ograniczenia dotyczące zapewniania mechanizmów wyboru, s. 11–12.

[121] UE: zob. dyrektywa 95/46, art. 14.

[122] APEC: zob. wymogi programowe, pyt. 14–16, s. 11–13.

17. Zautomatyzowane decyzje indywidualne

Elementy wspólne wymagane zarówno do zatwierdzenia BCR, jak i certyfikacji CBPR

Nie dotyczy

Elementy wymagane do zatwierdzenia BCR	Elementy wymagane do certyfikacji CBPR
<p>Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą zawierać zobowiązanie, zgodnie z którym żadna ocena ani żadna decyzja odnosząca się do osoby, której dane dotyczą, i mająca na nią istotny wpływ, nie będzie oparta wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych tej osoby, chyba, że decyzja ta^[123]:</p> <ul style="list-style-type: none">- zostanie podjęta w trakcie zawierania lub realizacji umowy, pod warunkiem że wnioski w sprawie zawarcia lub realizacji umowy, wniesiony przez osobę, której dane dotyczą, zostanie przyjęty, lub że istnieją odpowiednie sposoby zabezpieczenia jego uzasadnionych interesów, jak np. uregulowania umożliwiające mu przedstawienie swojego punktu widzenia; lub- jest dozwolona przez prawo, które określa również sposoby zabezpieczenia uzasadnionych interesów osoby, której dane dotyczą.	Nie dotyczy

Dokumenty odniesienia

[123] UE: zob. WP154, pkt 9, s. 6.

18. Bezpieczeństwo i poufność

Elementy wspólne wymagane zarówno do zatwierdzenia BCR, jak i certyfikacji CBPR

Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą zawierać wymóg, zgodnie z którym należy wdrożyć odpowiednie środki techniczne i organizacyjne w celu ochrony danych osobowych przed przypadkowym lub nielegalnym zniszczeniem lub przypadkową utratą, zmianą, niedozwolonym ujawnieniem lub dostępem, jak również przed wszelkimi innymi nielegalnymi formami przetwarzania^[124].

Środki takie muszą zapewniać poziom bezpieczeństwa odpowiedni do zagrożeń wynikających z przetwarzania danych oraz charakteru danych objętych ochroną^[125].

Elementy dodatkowe wymagane do zatwierdzenia BCR	Elementy dodatkowe wymagane do certyfikacji CBPR
Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą również zawierać wymóg, zgodnie z którym środki bezpieczeństwa należy wdrażać, uwzględniając stan wiedzy w tej dziedzinie oraz koszt realizacji ^[126] .	<p>Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą również zawierać wymóg, zgodnie z którym środki zabezpieczające powinny być poddawane przeglądowi okresowemu i ponownej ocenie^[127].</p> <p>Należy wdrożyć politykę w zakresie bezpieczeństwa informacji^[128] i politykę w zakresie bezpiecznego usuwania danych osobowych^[129].</p> <p>Należy wdrożyć środki zabezpieczające w celu wykrywania ataków, naruszeń lub innych niedopatrzeń w zakresie bezpieczeństwa, zapobiegania im i reagowania na nie^[130].</p> <p>Pracownicy muszą być także świadomi znaczenia utrzymywania bezpieczeństwa danych osobowych poprzez prowadzenie regularnych szkoleń i nadzoru określonych w procedurach, jak również znać obowiązki związane z utrzymywaniem tego bezpieczeństwa^[131].</p>

Dokumenty odniesienia

[124] UE: zob. dyrektywa 95/46, art. 17 ust. 1; WP108, pkt 8.2.4, s. 8; APEC: zob. ramowe zasady prywatności, część (iii), zasada VII, pkt 22, s. 2; kwestionariusz wstępny, pyt. 27, s. 14.

[125] UE: zob. dyrektywa 95/46, art. 17 ust. 1; APEC: zob. ramowe zasady prywatności, część (iii), zasada VII, pkt 22, s. 21; kwestionariusz wstępny, pyt. 28, s. 14.

[126] UE: zob. dyrektywa 95/46, art. art. 17 ust. 1.

- [127] APEC: zob. ramowe zasady prywatności, część (iii), zasada VII, pkt 22, s. 21.
- [128] APEC: zob. kwestionariusz wstępny, pyt. 26, s. 14.
- [129] APEC: zob. kwestionariusz wstępny, pyt. 31, s. 15.
- [130] APEC: zob. kwestionariusz wstępny, pyt. 32 i 33, s. 15.
- [131] APEC: zob. kwestionariusz wstępny, pyt. 29 i 30 lit. a), s. 14.

19. Program szkoleń

Elementy wspólne wymagane zarówno do zatwierdzenia BCR, jak i certyfikacji CBPR

Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą przewidywać odpowiednie szkolenia dla personelu organizacji w zakresie obowiązujących w niej zasad ochrony danych osobowych i prywatności^[132].

Elementy dodatkowe wymagane do zatwierdzenia BCR	Elementy dodatkowe wymagane do certyfikacji CBPR
Wymóg szkoleń dotyczy pracowników, którzy mają stały lub regularny dostęp do danych osobowych, uczestniczą w gromadzeniu danych osobowych lub uczestniczą w opracowywaniu narzędzi wykorzystywanych do przetwarzania danych osobowych ^[133] .	Szkolenia powinny obejmować politykę i procedury ochrony prywatności, w tym sposoby reagowania na skargi związane z ochroną prywatności ^[134] . Pracownicy muszą być także świadomi znaczenia utrzymywania bezpieczeństwa danych osobowych poprzez prowadzenie regularnych szkoleń i nadzoru określonych w procedurach, jak również znać obowiązki związane z utrzymywaniem tego bezpieczeństwa ^[135] .

Dokumenty odniesienia

[132] UE: zob. WP74, pkt 5.1, s. 16; APEC: zob. kwestionariusz wstępny, pyt. 44, s. 22.

[133] UE: zob. WP153, pkt 2.1, s. 5.

[134] APEC: zob. wymogi programowe, pyt. 44, s. 25–26.

[135] APEC: zob. kwestionariusz wstępny, pyt. 30 lit. a), s. 14.

20. Monitorowanie i program audytów

Elementy wspólne wymagane zarówno do zatwierdzenia BCR, jak i certyfikacji CBPR

Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą przewidywać monitorowanie stosowania i zgodności zasad organizacji dotyczących ochrony danych osobowych i prywatności[136].

Elementy dodatkowe wymagane do zatwierdzenia BCR	Elementy dodatkowe wymagane do certyfikacji CBPR
<p>W zasadach organizacji dotyczących ochrony danych osobowych i prywatności należy również określić obowiązek przeprowadzania audytu zgodności grupy z zasadami ochrony danych osobowych i prywatności, a w szczególności następujące obowiązki[137]:</p> <ul style="list-style-type: none">- program audytu musi obejmować wszystkie aspekty zasad ochrony danych osobowych i prywatności danej organizacji, w tym metody zapewniania, aby przeprowadzone zostały działania naprawcze;- audyt taki jest przeprowadzany regularnie (należy określić częstotliwość) przez wewnętrzny lub zewnętrzny akredytowany zespół audytowy lub na szczególny wniosek urzędnika ds. prywatności/osoby zajmującej się kwestią prywatności (lub jakiegokolwiek innej właściwej osoby w danej organizacji);- wyniki wszystkich audytów należy przekazywać urzędnikowi ds. prywatności/osobie zajmującej się kwestią prywatności (lub jakiegokolwiek innej właściwej osobie w danej organizacji) oraz zarządowi;- organy ochrony danych w UE mogą otrzymać kopię takiego audytu na wniosek;- w ramach planu audytu należy zapewnić organom ochrony danych w UE uprawnienia do przeprowadzenia, w	<p>Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą również zawierać wymóg, zgodnie z którym administrator danych co roku musi potwierdzać, czy organizacja nadal spełnia wymogi programowe CBPR[138].</p> <p>Pełnomocnicy APEC odpowiedzialni za rozliczalność będą przeprowadzali regularne kompleksowe przeglądy w celu zapewnienia integralności ponownej certyfikacji[139].</p> <p>Administrator danych przeprowadza regularne kontrole wyrywkowe lub monitoruje przetwarzających, pośredników, wykonawców lub innych dostawców usług wykorzystujących jego dane osobowe w celu zapewnienia zgodności z jego poleceniami lub uzgodnieniami/umowami[140].</p>

<p>razie potrzeby, audytu w zakresie ochrony danych;</p> <p>- każdy członek grupy musi zgodzić się na możliwość objęcia go audytem przez organy ochrony danych w UE oraz przestrzegać zaleceń organów ochrony danych w UE dotyczących jakichkolwiek kwestii związanych z tymi zasadami.</p>	
---	--

Dokumenty odniesienia

[136] UE: zob. WP74, pkt 5.2, s. 16; APEC: zob. wniosek o uznanie, załącznik A, pkt 6–8, s. 6.

[137] UE: zob. WP153, pkt 2.3, s. 7.

[138] APEC: zob. wniosek o uznanie, załącznik A, pkt 8, s. 6.

[139] APEC: zob. wniosek o uznanie, załącznik A, pkt 8, s. 6.

[140] APEC: zob. kwestionariusz wstępny, pyt. 49, s. 23.

21. Zgodność i nadzorowanie zgodności

Elementy wspólne wymagane zarówno do zatwierdzenia BCR, jak i certyfikacji CBPR

W zasadach organizacji dotyczących ochrony danych osobowych i prywatności przewiduje się wyznaczenie odpowiedniego personelu (np. sieci urzędników ds. ochrony prywatności) odpowiedzialnego za nadzór i zapewnianie zgodności z zasadami organizacji dotyczącymi ochrony danych osobowych i prywatności^[141].

Elementy dodatkowe wymagane do zatwierdzenia BCR^[142]	Elementy dodatkowe wymagane do certyfikacji CBPR
<p>Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą również zawierać krótki opis struktury wewnętrznej, roli i obowiązków sieci lub urzędników ds. ochrony prywatności, lub osób na podobnym stanowisku utworzonym w celu zapewnienia zgodności z zasadami organizacji dotyczącymi ochrony danych osobowych i prywatności.</p> <p>Wyznaczony odpowiedni personel otrzymuje wsparcie ze strony kadry kierowniczej wyższego szczebla.</p> <p>Przykład struktury wewnętrznej, roli i obowiązków sieci lub urzędników ds. ochrony prywatności lub osób na podobnym stanowisku utworzonym w celu zapewnienia zgodności z zasadami organizacji dotyczącymi ochrony danych osobowych i prywatności: główny urzędnik ds. ochrony prywatności doradza zarządowi, zajmuje się dochodzeniami prowadzonymi przez krajowe organy ochrony danych w UE, składa coroczne sprawozdania na temat zgodności, zapewnia zgodność na poziomie globalnym oraz powierza urzędnikom ds. ochrony prywatności zadanie polegające na rozpatrywaniu lokalnych skarg złożonych przez osoby, których dane dotyczą, informując głównego urzędnika ds. ochrony prywatności o poważnych kwestiach związanych z ochroną prywatności, oraz na zapewnianiu zgodności na poziomie lokalnym.</p>	<p>Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą również zawierać wymóg, zgodnie z którym wyznaczona osoba lub wyznaczone osoby wdrażają odpowiednie procedury dotyczące przyjmowania i analizowania skarg dotyczących ochrony prywatności oraz ustosunkowywania się do nich, wyjaśniając w stosownych przypadkach wszelkie działania zaradcze^[143].</p>

Dokumenty odniesienia

[141] UE: zob WP74, pkt 5.1, s. 16; APEC: zob. kwestionariusz wstępny, pyt. 40, s.21.

[142] UE: zob. WP153, pkt 2.4, s. 8.

[143] APEC: zob. wymogi programowe, pyt. 40, s. 24–25.

22. Wewnętrzne mechanizmy wnoszenia skarg

Elementy wspólne wymagane zarówno do zatwierdzenia BCR, jak i certyfikacji CBPR

W ramach zasad organizacji dotyczących ochrony danych osobowych i prywatności należy wprowadzić procedurę rozpatrywania skarg, zgodnie z którą^[144]:

- każda osoba, której dane dotyczą, może złożyć skargę w przypadku, gdy którykolwiek z członków grupy nie przestrzega zasad organizacji dotyczących ochrony danych osobowych i prywatności;
- skargi będą rozpatrywane przez wyraźnie określony wydział lub wyraźnie określoną osobę.

Elementy dodatkowe wymagane do zatwierdzenia BCR	Elementy dodatkowe wymagane do certyfikacji CBPR
Określony wydział rozpatrujący/osoba rozpatrująca skargi musi korzystać z wystarczającego stopnia niezależności podczas pełnienia swoich funkcji ^[145] .	Odpowiedź na skargę przekazywana osobom, których dane dotyczą, musi zawierać wyjaśnienie działania zaradczego podejmowanego w odniesieniu do skarg złożonych przez te osoby ^[146] .

Dokumenty odniesienia

[144] UE: zob. WP74, pkt 5.3, s. 17; APEC: zob. kwestionariusz wstępny, pyt. 41–42, s.21.

[145] UE: zob. WP74, pkt 5.3, s. 17.

[146] APEC: zob. kwestionariusz wstępny, pyt. 43, s. 21.

23. Aktualizacje zasad organizacji dotyczących ochrony danych osobowych i prywatności

Elementy wspólne wymagane zarówno do zatwierdzenia BCR, jak i certyfikacji CBPR

Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą zawierać wymóg zgłaszania wszelkich istotnych zmian wprowadzanych w ich treści lub w wykazie członków wszystkim członkom grupy, organom ochrony danych w UE i pełnomocnikom APEC odpowiedzialnym za rozliczalność w celu uwzględniania zmian w otoczeniu regulacyjnym i strukturze przedsiębiorstwa oraz dokładniej ze względu na fakt, iż niektóre zmiany mogą wymagać wydania nowych zezwoleń przez organy ochrony danych w UE lub dokonania przeglądu przez pełnomocników APEC odpowiedzialnych za rozliczalność^[147].

Elementy dodatkowe wymagane do zatwierdzenia BCR	Elementy dodatkowe wymagane do certyfikacji CBPR
<p>Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą również zawierać zobowiązanie do informowania osób, których dane dotyczą, o istotnych zmianach w treści zasad organizacji dotyczących ochrony danych osobowych i prywatności^[148].</p> <p>Aktualizacje zasad organizacji dotyczących ochrony danych osobowych i prywatności lub wykazu członków grupy podlegającym tym zasadom są możliwe bez konieczności ponownego składania wniosku o wydanie zezwolenia, pod warunkiem że^[149]:</p> <ul style="list-style-type: none">(i) wyznaczona osoba prowadzi w pełni zaktualizowany wykaz członków grupy oraz monitoruje i rejestruje wszelkie aktualizacje zasad organizacji dotyczących ochrony danych osobowych i prywatności oraz przekazuje potrzebne informacje osobom, których dane dotyczą, oraz krajowym organom ochrony danych w UE na ich wnioski;(ii) nowemu członkowi nie przekazuje się żadnych danych, dopóki nie będzie on w sposób skuteczny podlegał wiążącym zasadom ochrony danych osobowych i prywatności i nie będzie	<p>Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą również zawierać wymóg natychmiastowego przeprowadzenia przeglądu przez pełnomocnika APEC odpowiedzialnego za rozliczalność w przypadku wprowadzenia istotnej zmiany w treści zasad ochrony danych osobowych i prywatności (ustalonej zasadnie i w dobrej wierze przez pełnomocnika APEC odpowiedzialnego za rozliczalność)^[150].</p> <p>Organizacje powinny przekazywać aktualne oświadczenie w sprawie własnych praktyk i strategii dotyczących danych osobowych^[151].</p> <p>Organizacje dodatkowo są zobowiązane do zapewnienia osobom fizycznym mechanizmów wyboru w odniesieniu do gromadzenia, wykorzystywania i ujawniania danych osobowych tych osób^[152].</p>

<p>mógł zapewnić zgodności;</p> <p>(iii) informacje o zmianach zasad ochrony danych osobowych i prywatności lub wykazu członków są przekazywane raz w roku krajowym organom ochrony danych w UE wydającym zezwolenia wraz z krótkim wyjaśnieniem powodów uzasadniających daną aktualizację.</p>	
---	--

Dokumenty odniesienia

- [147] UE: zob. WP74, pkt 4.2, s. 15; APEC: zob. wniosek o uznanie, załącznik A, pkt 8, s. 6.
- [148] UE: zob. WP154, pkt 21, s. 9–10.
- [149] UE: zob. WP74, pkt 4.2, s. 15.
- [150] APEC: zob. wniosek o uznanie, załącznik A, pkt 8, s. 6.
- [151] APEC: zob. ramowe zasady prywatności, część (iii), zasada II, pkt 15; kwestionariusz wstępny, pyt. 1 s. 4.
- [152] APEC: zob. wymogi programowe, pyt. 14–16, s. 11–13.

24. Działania w przypadku ryzyka uniemożliwienia przez lokalne prawodawstwo zachowania zgodności z zasadami organizacji dotyczącymi ochrony danych osobowych i prywatności oraz w przypadku wniosków o udzielenie dostępu składanych przez organy ścigania

Elementy wspólne wymagane zarówno do zatwierdzenia BCR, jak i certyfikacji CBPR

Nie dotyczy

Elementy wymagane do zatwierdzenia BCR^[153]	Elementy wymagane do certyfikacji CBPR
<p>Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą zawierać przejrzyste postanowienie, że w przypadkach, w których członek grupy ma powody, by sądzić, iż obowiązujące przepisy uniemożliwiają mu wywiązywanie się z jego zobowiązań wynikających z zasad organizacji dotyczących ochrony danych osobowych i prywatności, a także mają istotny wpływ na udzielane w ich ramach gwarancje, członek ten musi niezwłocznie powiadomić siedzibę główną w UE lub członka grupy z siedzibą w UE, któremu przyznano obowiązki w zakresie ochrony danych, lub inną osobę zajmującą odpowiednie stanowisko w zakresie ochrony prywatności (o ile organ ścigania nie wydał w tym zakresie zakazu, na przykład na mocy prawa karnego w celu zachowania poufności postępowania prowadzonego przez organy ścigania).</p> <p>Ponadto zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą stanowić, że w przypadku konfliktu między przepisami prawa krajowego a obowiązkami, wymogami i zobowiązaniami przewidzianymi w zasadach organizacji dotyczących ochrony danych osobowych i prywatności z siedzibą główną w UE, członek grupy z siedzibą w UE, któremu przyznano obowiązki w zakresie ochrony danych lub inna osoba zajmująca odpowiednie stanowisko w zakresie ochrony prywatności muszą skonsultować się z właściwymi</p>	<p>Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą zawierać wymóg istnienia procedury postępowania w przypadku wezwań, nakazów lub postanowień, w tym wymagających ujawnienia danych osobowych, wydawanych przez organy sądowe lub inne organy rządowe^[154].</p>

<p>krajowymi organami ochrony danych w UE oraz podjąć odpowiedzialną decyzję w sprawie rodzaju działania, jakie należy podjąć.</p> <p>Wszelkie przypadki wymienione w niniejszym punkcie zasad organizacji dotyczących ochrony danych osobowych i prywatności będą szczegółowo omawiane i poddawane przeglądowi w ramach regularnie prowadzonych audytów, o których mowa w sekcji 20.</p>	
---	--

Dokumenty odniesienia

[153] UE: zob. WP74, pkt 3.3.3, s. 13–14 oraz WP154, pkt 16, s. 8.

[154] APEC: zob. kwestionariusz wstępny, pyt. 45, s. 22.

25. Wzajemna pomoc i współpraca z krajowymi organami ochrony danych w UE/organami egzekwowania ochrony prywatności APEC

Elementy wspólne wymagane zarówno do zatwierdzenia BCR, jak i certyfikacji CBPR

Nie dotyczy

Elementy wymagane do zatwierdzenia BCR	Elementy wymagane do certyfikacji CBPR
<p>Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą zawierać zobowiązanie, zgodnie z którym^[155]:</p> <ul style="list-style-type: none">- członkowie grupy współpracują ze sobą i pomagają sobie wzajemnie w rozpatrywaniu wniosku lub skargi osoby prywatnej lub w ramach dochodzeń lub śledztw prowadzonych przez organy ochrony danych w UE;- podmioty stosują się do zaleceń organów ochrony danych w UE w sprawie każdej kwestii dotyczącej interpretacji zasad organizacji dotyczących ochrony danych osobowych i prywatności.	<p>Organizacje z gospodarek uczestniczących mogą uzyskać certyfikację CBPR. Gospodarki uczestniczące mogą uczestniczyć w systemie CBPR wyłącznie wówczas, gdy ich organ egzekwowania ochrony prywatności przystąpił do porozumienia APEC dotyczącego współpracy w zakresie transgranicznego egzekwowania ochrony prywatności (CPEA)^[156].</p>

Dokumenty odniesienia

[155] UE: zob. WP74, pkt 5.4, s. 17.

[156] APEC: zob. statut wspólnego panelu nadzoru, pkt 2.2 ppkt (i), s. 15.

26. Związek między lokalnymi przepisami prawa i zasadami organizacji dotyczącymi ochrony danych osobowych i prywatności

Elementy wspólne wymagane zarówno do zatwierdzenia BCR, jak i certyfikacji CBPR

Nie dotyczy

Elementy wymagane do zatwierdzenia BCR	Elementy wymagane do certyfikacji CBPR
<p>W przypadkach, w których dane osobowe są przetwarzane w UE, konieczne jest stosowanie unijnych przepisów o ochronie danych. Zasady organizacji dotyczące ochrony danych osobowych i prywatności muszą zatem zawierać potwierdzenie, zgodnie z którym^[157]:</p> <ul style="list-style-type: none">- w sytuacji, gdy zgodnie z prawodawstwem lokalnym, na przykład prawodawstwem UE, wymaga się wyższego poziomu ochrony danych osobowych, wówczas będzie ono nadrzędne wobec zasad organizacji dotyczących ochrony danych osobowych i prywatności;- w każdym przypadku dane należy przetwarzać zgodnie z prawem odpowiedniego państwa członkowskiego w myśl art. 4 dyrektywy 95/46/WE.	<p>Nie dotyczy</p>
<p>Wyjaśnienie związku między przepisami prawa lokalnego i BCR</p> <p>Nie dotyczy</p>	<p>Wyjaśnienie związku między lokalnymi przepisami prawa i CBPR^[158]</p> <p>Uczestnictwo w systemie CBPR nie zwalnia organizacji uczestniczącej ze zobowiązań prawnych wynikających z prawa krajowego.</p> <p>W przypadku braku mających zastosowanie wymogów krajowych dotyczących ochrony prywatności w danej gospodarce, zasady organizacji dotyczące ochrony danych osobowych mają na celu zapewnienie minimalnego poziomu ochrony.</p> <p>W przypadku gdy zakres krajowych</p>

	<p>wymogów prawnych wykracza poza oczekiwania określone w ramach zasad organizacji dotyczących ochrony danych osobowych i prywatności, zastosowanie mają nadal wspomniane krajowe przepisy ustawowe i wykonawcze w pełnym zakresie.</p> <p>W przypadku gdy zakres wymogów przewidzianych w ramach zasad organizacji dotyczących ochrony danych osobowych i prywatności wykracza poza zakres wymogów krajowych przepisów ustawowych i wykonawczych, organizacja będzie musiała spełnić takie dodatkowe wymogi, aby uczestniczyć w systemie.</p> <p>Organy egzekwowania ochrony prywatności w danej gospodarce powinny jednak mieć możliwość podejmowania działań w zakresie egzekwowania ochrony na mocy obowiązujących przepisów ustawowych i wykonawczych, które skutkują zapewnieniem ochrony danych osobowych zgodnie z wymogami programowymi CBPR.</p>
--	--

Dokumenty odniesienia

[157] UE: zob. WP74, pkt 3.3.3, s. 13–14.

[158] APEC: zob. strategie polityczne, zasady i wytyczne, pkt 43 i 44, s. 10–11.

27. Przepisy końcowe

Elementy wspólne wymagane zarówno do zatwierdzenia BCR, jak i certyfikacji CBPR

W zasadach organizacji dotyczących ochrony danych osobowych i prywatności należy określić datę ich wejścia w życie^[159].

Dokumenty odniesienia

[159] UE: zob. WP154, pkt 23, s. 10; APEC: zob. wymogi programowe, pyt. 1, s. 2.

Sporządzono w Brukseli dnia 27 lutego
2014 r.

*W imieniu Grupy Roboczej
Przewodniczący
Jacob KOHNSTAMM*

Dodatki

Dodatek 1. Dokumenty składane przez organizację ubiegającą się o zatwierdzenie jej BCR przez krajowe organy ochrony danych w UE oraz przez organizację ubiegającą się o uzyskanie certyfikacji jej CBPR przeprowadzanej przez pełnomocników APEC odpowiedzialnych za rozliczalność

Dodatek 1. Dokumenty składane przez organizację ubiegającą się o zatwierdzenie jej BCR przez krajowe organy ochrony danych w UE oraz przez organizację ubiegającą się o uzyskanie certyfikacji jej CBPR przeprowadzanej przez pełnomocników APEC odpowiedzialnych za rozliczalność

Organizacja ubiegająca się o zatwierdzenie jej BCR i uzyskanie certyfikacji jej CBPR przekazuje krajowym organom ochrony danych w UE i pełnomocnikowi APEC odpowiedzialnemu za rozliczalność dokumenty potwierdzające przestrzeganie zobowiązań i wymogów określonych w zasadach organizacji dotyczących ochrony danych osobowych i prywatności, na przykład^[160]:

- dokument dotyczący polityki ochrony prywatności (np. polityki ochrony prywatności klienta, polityki ochrony prywatności w dziale zasobów ludzkich) mający celu informowanie osób, których dane dotyczą, o stosowanym przez przedsiębiorstwo sposobie ochrony ich danych osobowych^[161];
- wytyczne dla pracowników mających dostęp do danych osobowych służące ułatwianiu zrozumienia i stosowania zasad przewidzianych w zasadach ochrony prywatności (np. wytyczne dotyczące tego, jak odpowiadać na skargę osoby, której dane dotyczą, w jaki sposób przekazywać informacje osobom, których dane dotyczą, oraz na temat odpowiednich środków bezpieczeństwa/poufności, których należy przestrzegać)^[162];
- przykłady lub objaśnienie programu szkoleniowego^[163];
- opis wewnętrznego systemu rozpatrywania skarg^[164];
- polityka bezpieczeństwa w zakresie systemów IT służących do przetwarzania danych osobowych UE i APEC^[165];
- wszelkie standardowe umowy, jakie mają być zawierane z przetwarzającymi (będącymi lub niebędącymi członkami grupy), którzy w stosownych przypadkach zajmują się przetwarzaniem danych osobowych UE i danych osobowych APEC^[166].

Elementy dodatkowe wymagane do zatwierdzenia BCR	Elementy dodatkowe wymagane do certyfikacji CBPR
Ponadto organizacja wnioskująca przekazuje krajowym organom ochrony danych w UE: <ul style="list-style-type: none">- opis stanowiska pracy inspektorów ochrony danych lub innych osób odpowiedzialnych za ochronę danych w przedsiębiorstwie;- standardowy formularz wniosku	Ponadto organizacja wnioskująca przekazuje pełnomocnikom APEC odpowiedzialnym za rozliczalność: <ul style="list-style-type: none">- kwestionariusz wstępny;- przykłady dokumentów dodatkowych, które mogą być potrzebne pełnomocnikom APEC odpowiedzialnym

<p>WP133^[167];</p> <ul style="list-style-type: none"> - plan i program audytu dotyczącego ochrony danych uzgodnione z właściwymi osobami (wewnętrznymi/zewnętrznymi akredytowanymi audytorami przedsiębiorstwa); - dokumenty potwierdzające, że członek, który jest źródłem przekazanych danych i posiada siedzibę poza UE, oraz siedziba główna w UE albo członek grupy w UE, któremu przekazano odpowiedzialność, dysponują wystarczającymi środkami do wypłaty odszkodowania za szkody powstałe w wyniku naruszenia zasad organizacji dotyczących ochrony danych osobowych i prywatności. 	<p>za rozliczalność do przeprowadzenia przeglądu zasad organizacji dotyczących ochrony danych osobowych i prywatności:</p> <ul style="list-style-type: none"> - przykłady zawiadomień przekazywanych osobom, których dane dotyczą^[168]; - dokumenty potwierdzające zgodność z ograniczeniem dotyczącym gromadzenia danych z podaniem^[169]: <ul style="list-style-type: none"> (i) każdego rodzaju zgromadzonych danych; (ii) odpowiedniego, określonego celu gromadzenia każdego rodzaju danych; oraz (iii) wszystkich sposobów wykorzystania mających zastosowanie do każdego rodzaju danych; (iv) wyjaśnienia zgodności i związku każdego określonego sposobu wykorzystania z określonym celem gromadzenia; - dokumenty potwierdzające, że dane są gromadzone, wykorzystywane i ujawniane w określonych celach lub innych zgodnych lub powiązanych celach, chyba że ma to miejsce na podstawie zgody wydanej w określonych okolicznościach^[170]; - dokumenty potwierdzające mechanizmy udostępnione osobom, których dane dotyczą, umożliwiające im dokonanie wyboru w odniesieniu do gromadzenia, wykorzystywania i ujawniania ich danych osobowych oraz potwierdzające istnienie i działanie takich mechanizmów, wraz z wyraźnym określeniem celu ich gromadzenia^[171]; - procedury wdrożone w celu potwierdzenia i zapewnienia, że
---	--

	<p>przechowywane dane osobowe są aktualne, prawidłowe i pełne w zakresie niezbędnym do realizacji celów ich wykorzystywania^[172];</p> <p>- dokumenty potwierdzające istnienie porozumień z przetwarzającymi, pełnomocnikami, wykonawcami lub innymi dostawcami usług, aby zapewnić wywiązywanie się administratora ze zobowiązań wobec osoby, której dane dotyczą^[173].</p>
--	---

Dokumenty odniesienia

[160] UE: zob. WP154, dokumenty składane w organach ochrony danych, s.10–11.

[161] APEC: zob. wymogi programowe, pyt. 1, s. 2–4.

[162] APEC: zob. wymogi programowe, pyt. 29, s.18; pyt. 44, s. 25–26.

[163] APEC: zob. wymogi programowe, pyt. 44, s. 25–26.

[164] APEC: zob. wymogi programowe, pyt. 41–43, s. 25.

[165] APEC: zob. wymogi programowe, pyt. 26, s.17; pyt. 31, s. 19.

[166] APEC: zob. wymogi programowe, pyt. 46, s. 26–27.

[167] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp133_en.doc

[168] APEC: zob. wymogi programowe, pyt. 2, s. 4.

[169] APEC: zob. wymogi programowe, pyt. 6, s. 6.

[170] APEC: zob. wymogi programowe, pyt. 8, s. 8.

[171] APEC: zob. wymogi programowe, pyt. 14–17, s. 11–13.

[172] APEC: zob. wymogi programowe, pyt. 21, s. 15.