Wersja 2.0

Obowiązuje od dnia:
10-04-2018

Standard ochrony prywatności w Allianz (SOPA)

Klasyfikacja: Dokument wewnętrzny

Autoryzacja:

Treść niniejszego dokumentu została zweryfikowana i zatwierdzona w następujący sposób:

Wersja	**Obowiązuje od dnia**	**Autoryzowany przez:**			**Przyjęta przez:**
		Zespół Grupy ds. Polityki	Członek Zarządu Allianz SE	Komitet Zarządu	Zarząd Allianz SE
1.0	10-04-2018	-	**Dr. Helga Jung** **13-04-2018**		[●]

Allianz

Streszczenie

I. Allianz jest silnie zaangażowany w prowadzenie działalności przy pełnym poszanowaniu i w zgodności ze stosownymi przepisami i regulacjami *w* zakresie prywatności i ochrony danych, a postępując w ten sposób, stara się zabezpieczyć Dane Osobowe Osób Fizycznych, chronić Grupę Allianz i promować Allianz jako godnego zaufania dostawcę produktów i usług finansowych.

II. Ramy prywatności i ochrony danych w Allianz obejmują:

- Niniejszy Standard ochrony prywatności w Allianz („SOPA") zawierający minimalne wymogi globalne mające zastosowanie do Grupy Allianz w zakresie Przetwarzania i przekazywania Danych Osobowych w obrębie Grupy Allianz, jak również wymogi dodatkowe wobec Przetwarzania Danych w EOG i Przekazywania Danych zgodnie z WRK. Jako taki, niniejszy SOPA stanowi, między innymi, prawnie uznany i stosowany w Allianz mechanizm legalizacji i umożliwiania transgranicznego przekazywania Danych Osobowych pochodzących z EOG lub tam przetwarzanych w ramach Grupy Allianz („Wiążące Reguły Korporacyjne" lub „WRK"); oraz
- Zasady funkcjonalne bardziej szczegółowo określające wymogi co do prywatności i ochrony danych, np. odnośnie dokonywania Ocen Wpływu na Prywatność czy też dokumentowania operacji przetwarzania danych

III. Niniejszy SOPA ma zastosowanie do Grupy Allianz. Dokument ten nie obejmuje kwestii bezpieczeństwa informacji, przechowywania dokumentacji, zarządzania incydentami ani ogólnej ochrony tajemnic handlowych, które podlegają wymogom innych standardów obowiązujących w Allianz.

IV. Zarząd Allianz SE przyjął niniejszy SOPA w kwietniu 2018 roku i wymaga prawnego związania wszystkich Podmiotów OE i Pracowników jego wymogami. Niniejszy SOPA jest prawnie wiążący dla podmiotów prawnych Grupy Allianz, które zamierzają zawrzeć Umowę Międzyzakładową.

V. Podmioty OE mogą opracować równoważne zasady i procedury mające na celu dostosowanie wymogów niniejszego SOPA, stosownie, do ich struktury lub modelu biznesowego. Wszelkie istotne odchylenia od niniejszego SOPA muszą zostać zakomunikowane Działowi Prywatności i Ochrony Danych Grupy i wcześniej z nim uzgodnione, a także właściwie udokumentowane.

VI. Niniejszy SOPA opiera się na wydzielonej odpowiedzialności członka Zarządu Allianz SE kierującego działem handlowym H6 i odpowiedzialnego za przestrzeganie prywatności i ochrony danych.

Spis treści

Akapit	Nagłówek	Str.
A.	**Wprowadzenie**	**5**
A.I.	Uzasadnienie	5
A.II.	Uprawnienia i aktualizacje	6
B.	**Zasady przestrzegania prywatności i ochrony danych**	**7**
B.I.	Należyta staranność	7
B.II.	Jakość danych	7
B.III.	Przejrzystość i otwartość	8
B.IV.	Legalność przetwarzania danych	10
B.V.	Stosunki z podmiotami przetwarzającymi dane	12
B.VI.	Przekazywanie danych i dalsze przekazywanie danych	12
B.VII.	Bezpieczeństwo i poufność danych	13
B.VIII.	Utrata danych osobowych	14
B.IV.	Ochrona prywatności w fazie projektowania I domyślna ochrona prywatności	15
B.X.	Współpraca z właściwymi organami ochrony danych działającymi na terenie EOG w zakresie przetwarzania danych w EOG i przekazywania danych zgodnie z WRK	16
C.	**Czynności i procesy dotyczące przestrzegania prywatności i ochrony danych**	**17**
C.I.	Dokumentacja operacji przetwarzania danych	17
C.II.	Szkolenia	17
C.III.	Wewnętrzny mechanizm rozpatrywania skarg	17
C.IV.	Ocena wpływu na prywatność (PIA)	18
C.V.	Monitorowanie i zapewnienie zgodności	18
D	**Obowiązki wobec osób fizycznych**	**19**
D.I.	Udzielanie odpowiedzi na wnioski osób fizycznych o uzyskanie dostępu, sprostowanie lub usunięcie danych	19
D.II.	Udzielanie odpowiedzi na wnioski osób fizycznych dot. sprzeciwu wobec przetwarzania danych w EOG i przekazywania danych zgodnie z WRK	20
D.III.	Udzielanie odpowiedzi na wnioski osób fizycznych o ograniczenie przetwarzania danych w EOG i przekazywania danych zgodnie z WRK	21
D.IV.	Udzielanie odpowiedzi na wnioski osób fizycznych o umożliwienie przenoszalności danych odnośnie przetwarzania danych w EOG i przekazywanie danych zgodnie z WRK	22

D. V.	Udzielanie odpowiedzi na wnioski osób fizycznych dotyczące sprzeciwu wobec zautomatyzowanych decyzji w sprawie przetwarzania danych w EOG i przekazywania danych zgodnie z WRK	22

E.	**Podział ról i obowiązków**	**24**
E.I.	Poziom Grupy Allianz	24
E.II.	Poziom podmiotów OE Allianz	26
E.III.	Grupa Allianz i kierowanie podmiotami OE	30
F.	**Odniesienia do innych dokumentów**	31
	Załączniki	
Załącznik A	Słownik terminów	**32**
Załącznik B	Przekazywanie danych zgodnie z WRK objęte niniejszym SOPA	**35**
Załącznik C	Wymogi minimalne odnośnie umów zawieranych między administratorem danych a podmiotem przetwarzającym dane o przetwarzanie danych w EOG i przekazywanie danych zgodnie z WRK	**37**
Załącznik D	Rozpatrywanie wniosków osób fizycznych dotyczących przetwarzania danych w EOG oraz skarg dotyczących przekazywania danych zgodnie z WRK	**39**
Załącznik E	Przegląd wymogów zawartych w SOPA	**42**

A. Wprowadzenie

I. Uzasadnienie

1. Allianz angażuje się w ochronę prawa do prywatności i ochrony danych swoich Pracowników, klientów, partnerów handlowych i stron trzecich („Osób Fizycznych"). Niniejszy Standard ochrony prywatności w Allianz („SOPA") ma na celu umożliwienie przestrzegania stosownych przepisów i regulacji w zakresie prywatności i ochrony danych regulujących Przetwarzanie i przekazywanie Danych Osobowych. W szczególności, niniejszy SOPA zapewnia ramy dla Danych Osobowych podlegających przepisom i regulacjom EOG w obrębie Grupy Allianz oraz odpowiednie zabezpieczenia wobec Danych EOG przekazywanych do podmiotów OE spoza EOG, bardziej szczegółowo określonych w Załączniku B. Jako taki, niniejszy SOPA stanowi, między innymi, prawnie uznany i stosowany w Allianz mechanizm legalizacji i umożliwiania przekazywania Danych Osobowych pochodzących z EOG lub tam przetwarzanych w ramach Grupy Allianz („Wiążące Reguły Korporacyjne" lub „WRK").

2. Niniejszy SOPA określa globalne minimalne wymogi w zakresie prywatności i ochrony danych odnośnie Przetwarzania Danych Osobowych przez wszystkie Podmioty OE („Globalne wymogi minimalne", ikona nr 1 poniżej). Ponadto, SOPA przedstawia wymogi minimalne dotyczące Przetwarzania Danych Osobowych podlegających przepisom i regulacjom obowiązującym w EOG („Wymogi wobec przetwarzania danych w EOG", ikona nr 2 poniżej) oraz transgranicznego przekazywania Danych Osobowych podlegających przepisom i regulacjom obowiązującym w EOG zachodzącego w obrębie Grupy Allianz („Wymogi wobec przekazywania danych zgodnie z WRK", ikona nr 3 poniżej). Wymogi wobec przetwarzania danych w EOG oraz Wymogi wobec przekazywania danych zgodnie z WRK mają zastosowanie jako dodatek do Globalnych wymogów minimalnych. W niniejszym SOPA poniższe ikony mają następujące znaczenie:

   
   Stosuje się do Przetwarzania Danych Osobowych w ogóle („Globalne wymogi minimalne")

   
   Stosuje się do Przetwarzania Danych Osobowych podlegających przepisom regulacjom obowiązującym w EOG („Wymogi wobec przetwarzania danych w EOG")

   
   Stosuje się do Danych EOG przekazywanych w obrębie Grupy Allianz („Wymogi wobec przekazywania danych zgodnie z WRK").

   Dla ułatwienia Załącznik E (Przegląd wymogów zawartych w SOPA) obejmuje zarys wszystkich wymogów).

3. Niniejszy SOPA zastępuje Standard ochrony i prywatności danych w Allianz z dnia 1 października 2013 roku. Niniejszy SOPA może zostać uzupełniony o Zasady funkcjonalne. Niniejszy SOPA i odpowiednie Zasady funkcjonalne razem tworzą Ramy prywatności i ochrony danych w Allianz („Ramy"),

4. Niniejszy SOPA ma zastosowanie do Grupy Allianz i wymaga prawnego związania wszystkich Podmiotów OE i Pracowników jego wymogami. Niniejszy SOPA jest prawnie wiążący dla podmiotów prawnych Grupy Allianz, które zamierzają zawrzeć Umowę Międzyzakładową.

5. Podmioty OE muszą skutecznie wdrożyć Ramy zgodnie z wymogami prawnymi ich jurysdykcji i przedstawić Ramy wszystkim stosownym adresatom.

6. Niniejszy SOPA nie obejmuje kwestii bezpieczeństwa informacji, przechowywania dokumentacji, zarządzania incydentami ani ogólnej ochrony tajemnic handlowych, które podlegają wymogom innych standardów obowiązujących w Allianz.
7. Jeżeli jakakolwiek część niniejszego SOPA jest mniej rygorystyczna niż lokalne przepisy lub regulacje, pierwszeństwo zachowują lokalne przepisy lub regulacje. W razie jakiejkolwiek rozbieżności pomiędzy Globalnymi wymogami minimalnymi a Wymogami wobec przetwarzania danych w EOG i Wymogami wobec przekazywania danych zgodnie z WRK zawartymi w niniejszym SOPA, pierwszeństwo zachowują Wymogi wobec przetwarzania danych w EOG i Wymogi wobec przekazywania danych zgodnie z WRK. W razie niepewności Specjalista ds. Prywatności Danych/Inspektor Ochrony Danych poszczególnego Podmiotu OE musi skonsultować się z Działem Prywatności i Ochrony Danych Grupy w celu rozwiązania konfliktu.

II. Uprawnienia i aktualizacje

Całkowita odpowiedzialność za Dział Prywatności i Ochrony Danych Grupy spoczywa na członku Zarządu Allianz SE kierującym działem handlowym H6. Dział Prywatności i Ochrony Danych Grupy jest właścicielem niniejszego SOPA i powierzono mu odpowiedzialność za utrzymanie i aktualizacji SOPA. Niniejszy SOPA podlega weryfikacji przynajmniej raz na rok. Niniejszy SOPA musi być zatwierdzony przez członka Zarządu Allianz SE kierującego działem handlowym H6 i należycie odnotowany przez Zarząd Allianz SE.

Ramy i aktualny wykaz podmiotów prawnych Grupy Allianz, które zawarły Umowę Międzyzakładową, są dostępne na Allianz Connect, Księga reguł korporacyjnych. Publiczna wersja niniejszego SOPA, obejmująca streszczenie SOPA, wymogi egzekwowalne dla Osób Fizycznych oraz procedurę rozpatrywania skarg opisaną w Załączniku D, Dział II, a także aktualny wykaz podmiotów prawnych Grupy Allianz, które zawarły Umowę Międzyzakładową, są dostępne na stronie www.allianz.com.

Niniejszy SOPA wchodzi w życie w dniu jego przedstawienia Zarządowi Allianz SE. W zakresie, w jakim znajduje to zastosowanie, Podmioty OE muszą zacząć stosować niniejszy SOPA do dnia 24 maja 2018 roku. Niniejszy SOPA zastępuje Standard ochrony i prywatności danych w Allianz z dnia 1 października 2013 roku.

B. Zasady przestrzegania prywatności i ochrony danych

I. Należyta staranność

Podmioty OE działające jako Administratorzy Danych są zobowiązani do Przetwarzania Danych Osobowych z należytą starannością, zgodnie z prawem, uczciwie i w przejrzysty sposób w odniesieniu do Osób Fizycznych.

II. Jakość danych

1. Ograniczenie celu

1.1. Globalne wymogi minimalne

Podmioty OE działające jako Administratorzy Danych są zobowiązani do Przetwarzania Danych Osobowych dla określonych, jednoznacznych i uzasadnionych celów biznesowych i zgodnie ze stosownymi przepisami i regulacjami, obejmującymi tajemnicę zawodową, a także minimalnymi wymogami Allianz odnośnie bezpieczeństwa informacji określonymi w Standardzie bezpieczeństwa informacji w Allianz i towarzyszących mu Dyrektywach bezpieczeństwa informacji w Allianz, jak również wymogami odnośnie przechowywania danych zawartymi w Standardzie zarządzania dokumentami w Allianz.

Podmioty OE muszą Przetwarzać Dane Osobowe wyłącznie w zakresie, w jakim jest to niezbędne dla realizacji określonych celów biznesowych.

Podmioty OE mogą wprowadzać późniejsze zmiany w określonych celach biznesowych pod warunkiem, że takie zmiany są określone, jednoznaczne i uzasadnione.

1.2. Wymogi dodatkowe wobec przetwarzania danych w EOG i przekazywania danych zgodnie z WRK

Podmioty OE działające jako Administratorzy Danych mogą wprowadzać późniejsze zmiany w określonych celach biznesowych, jeżeli nie są one sprzeczne z celami pierwotnymi.

2. Minimalizacja i dokładność danych

Podmioty OE działające jako Administratorzy Danych muszą zapewnić:

- Aktualizację Danych Osobowych oraz bezzwłoczne usunięcie lub sprostowanie wszelkich nieścisłości, mając na uwadze cele, dla których są one Przetwarzane;
- Uwzględnienie wszelkich aktualizacji Danych Osobowych we wszystkich, wewnętrznych i zewnętrznych, systemach i bazach danych; oraz
- Dokładność Danych Osobowych i ich ograniczenie do treści niezbędnej dla celów, dla których są one Przetwarzane.

3. Ograniczenie przechowywania

Podmioty OE działające jako Administratorzy Danych muszą przechowywać Dane Osobowe tak długo, jak jest to niezbędne dla realizacji określonych celów biznesowych lub wymagane przez stosowne przepisy i regulacje, oraz zgodnie z wymogami Allianz odnośnie przechowywania danych zawartymi w Standardzie zarządzania dokumentami w Allianz.

Podmioty OE działające jako Administratorzy Danych są zobowiązane do właściwej utylizacji i archiwizacji Danych Osobowych zgodnie ze stosownymi przepisami i regulacjami oraz wymogami Allianz odnośnie przechowywania danych zawartymi w Standardzie zarządzania dokumentami w Allianz.

Podmioty OE działające jako Administratorzy Danych zamiast utylizacji mogą zanonimizować Dane Osobowe.

III. Przejrzystość i otwartość

1. Globalne wymogi minimalne

Podmioty OE działające jako Administratorzy Danych muszą, zgodnie ze stosownymi przepisami i regulacjami, w czasie gromadzenia danych i w jasny i przystępny sposób, poinformować Osoby Fizyczne o celach, dla których gromadzone są Dane Osobowe, o sposobie, w jaki mają być one Przetwarzane, i, jeśli dotyczy, o osobach, którym zostaną one przekazane.

Podmioty OE działające jako Administratorzy Danych muszą zapewnić, że Dane Osobowe będą zbierane głównie bezpośrednio od Osoby Fizycznej, której one dotyczą, oraz, że będą zbierane od stron trzecich lub od innych źródeł pod warunkiem, że jest to uzasadnione i dozwolone przez stosowne przepisy i regulacje.

2. Wymogi dodatkowe wobec przetwarzania danych w EOG i przekazywania danych zgodnie z WRK

2.1. Informacje zbierane od osób fizycznych

Podmioty OE działające jako Administratorzy Danych muszą przekazać Osobom Fizycznym, na piśmie lub w inny sposób, obejmujący, w stosownych przypadkach, formę elektroniczną, informacje przedstawione poniżej. Następujące informacje muszą zostać podane w sposób zwięzły i przejrzysty, w łatwo dostępnej formie i w jasnym i prostym języku:

- Nazwa i dane kontaktowe Podmiotu OE działającego jako Administrator Danych lub jego przedstawiciel;
- Dane kontaktowe Specjalisty ds. Prywatności Danych/Inspektora Ochrony Danych Podmiotu OE w stosownych przypadkach;
- Planowane cele Przetwarzania Danych Osobowych oraz podstawy prawne ich Przetwarzania;
- Uzasadnione interesy Administratora Danych lub strony trzeciej, gdy takie interesy zapewniają podstawę prawną dla Przetwarzania Danych;
- Odbiorcy lub kategorie odbiorców Danych Osobowych;
- W przypadku przekazywania danych do krajów spoza EOG - zabezpieczenia wdrożone w celu ochrony przekazywanych Danych Osobowych oraz sposób, w jaki Osoba Fizyczna może uzyskać ich kopię lub informację, gdzie dane zostały udostępnione;
- Okres przechowywania Danych Osobowych lub, jeśli nie jest to możliwe, kryteria stosowane w celu ustalenia tego okresu;
- Istnienie prawa Osób Fizycznych do:
  - Uzyskania dostępu, sprostowania i usunięcia Danych Osobowych;
  - Ograniczenia Przetwarzania Danych;
  - Przenoszalności danych;

- Zgłoszenia sprzeciwu wobec Przetwarzania Danych. Prawo to musi zostać wyraźnie zakomunikowane Osobie Fizycznej, w jasny sposób i oddzielnie od wszelkich innych informacji, gdy Przetwarzanie opiera się na uzasadnionych interesach Administratora Danych lub gdy Dane Osobowe są Przetwarzane w celach marketingu bezpośredniego;
- Wycofania zgody w każdym czasie, gdy zapewnia ona podstawę prawną dla Przetwarzania Danych Osobowych lub Wrażliwych Danych Osobowych. Takie wycofanie zgody nie wpływa na legalność Przetwarzania Danych prowadzonego przed złożeniem przez Osobę Fizyczną wniosku o wycofanie zgody; oraz
- Zgłoszenia skargi do właściwego organu ochrony danych działającego na terenie EOG;

- Informacje, czy przekazanie Danych Osobowych stanowi wymóg ustawowy lub umowny lub niezbędny do zawarcia umowy oraz informacje, czy Osoba Fizyczna jest zobowiązana do przekazania Danych Osobowych, a także możliwe konsekwencje nieprzekazania danych; oraz
- Istnienie zautomatyzowanego procesu podejmowania decyzji obejmującego Profilowanie, a także istotne informacje dotyczące zastosowanej logiki oraz znaczenie i przewidywane konsekwencje takiego Przetwarzania Danych dla Osoby Fizycznej.

Podmioty OE działające jako Administratorzy Danych zamierzający Przetwarzać Dane Osobowe w celu innym niż cel pierwotny muszą, przed dalszym Przetwarzaniem Danych, podać Osobom Fizycznym, których to dotyczy, taki inny cel oraz wszelkie inne istotne informacje wymienione powyżej.

2.2. Informacje nie zbierane od osób fizycznych

W przypadkach gdy Dane Osobowe nie są uzyskiwane od Osób Fizycznych, Podmioty OE działające jako Administratorzy Danych muszą, poza informacjami wymienionymi w Rozdziale B, Dział III. ust. 2 pkt. 2.1 powyżej, dostarczyć im poniższe informacje:

- Kategorie Danych Osobowych, których to dotyczy; oraz
- Źródło Danych Osobowych i, jeżeli dotyczy, informację, czy pochodzą one z publicznie dostępnych źródeł.

Podmioty OE działające jako Administratorzy Danych muszą przekazać Osobom Fizycznym powyższe informacje:

- W ciągu 1 miesiąca od uzyskania Danych Osobowych z uwzględnieniem szczególnych okoliczności Przetwarzania Danych Osobowych;
- Jeżeli Dane Osobowe mają być wykorzystywane w celu komunikacji z Osobą Fizyczną, której dotyczą Dane Osobowe - najpóźniej w czasie pierwszego kontaktu z taką Osobą Fizyczną; lub
- Jeśli przewidywane jest ujawnienie danych innemu odbiorcy - najpóźniej z chwilą pierwszego ujawnienia Danych Osobowych.

Podmioty OE działające jako Administratorzy Danych zamierzający Przetwarzać Dane Osobowe w celu innym niż cel pierwotny muszą, przed dalszym Przetwarzaniem Danych, podać Osobom Fizycznym, których to dotyczy, taki inny cel oraz wszelkie inne istotne informacje wymienione powyżej.

Podmioty OE działające jako Administratorzy Danych nie muszą przekazać Osobom Fizycznym powyższych informacji, jeżeli:

- Są one już w posiadaniu takich informacji;

- Okazałoby się to niemożliwe lub wiązałoby się to z niewspółmiernym wysiłkiem;
- Stosowne przepisy i regulacje obowiązujące w EOG wyraźnie wymagają uzyskania lub ujawnienia Danych Osobowych; lub
- Dane Osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej wymaganym w stosownych przepisach i regulacjach obowiązujących w EOG.

IV. Legalność przetwarzania danych

1. Globalne wymogi minimalne

Podmioty OE działające jako Administratorzy Danych mogą przetwarzać Dane Osobowe wyłącznie, jeżeli istnieje jedna z poniższych podstaw prawnych:

- Przetwarzanie Danych jest niezbędne w celu realizacji umowy, której stroną jest Osoba Fizyczna lub w celu podjęcia kroków na prośbę Osoby Fizycznej przed zawarciem umowy;
- Przetwarzanie Danych jest niezbędne dla przestrzegania obowiązku prawnego, któremu podlega Administrator Danych;
- Przetwarzanie Danych jest niezbędne dla ochrony żywotnych interesów Osoby Fizycznej lub innej osoby fizycznej;
- Przetwarzanie Danych jest niezbędne dla wykonania zadania w interesie publicznym lub wykonywania oficjalnych uprawnień powierzonych Administratorowi Danych;
- Przetwarzanie Danych jest niezbędne dla uzasadnionych interesów Administratora Danych lub strony trzeciej, poza sytuacją, gdy charakter nadrzędny w stosunku do takich uzasadnionych interesów mają interesy Osoby Fizycznej lub podstawowe prawa i wolności wymagające ochrony, lub
- Osoba Fizyczna udzieliła zgody na warunkach określonych w Dziale IV ust. 2 poniżej.

2. Warunki udzielenia zgody na przetwarzanie danych w EOG i przekazywanie danych zgodnie z WRK

W przypadkach gdy Dane Osobowe są Przetwarzane na podstawie zgody Osoby Fizycznej Podmioty OE działające jako Administratorzy Danych muszą:

- Zapewnić, że zgoda jest dobrowolna, konkretna i świadoma i stanowi jednoznaczne wskazanie zamiaru Osoby Fizycznej (wyrażonego stwierdzeniem lub wyraźnym działaniem potwierdzającym) udzielenia zgody na Przetwarzanie Danych;
- Zapewnić, że Osoba Fizyczna może w łatwy sposób wycofać swoją zgodę i otrzyma informację o takiej możliwości przed udzieleniem zgody;
- Wdrożyć i utrzymywać procesy rejestracji udzielenia lub wycofania zgody; oraz
- Zapewnić, że jeśli zgoda jest udzielana w ramach pisemnego oświadczenia dotyczącego również innych spraw, jest przedstawiona w sposób wyraźnie odróżniający się od innych kwestii w zrozumiałej formie i w jasnym i prostym języku.

3. Legalność przetwarzania wrażliwych danych osobowych w przypadku przetwarzania danych w EOG i przekazywania danych zgodnie z WRK

Podmioty OE działające jako Administratorzy Danych muszą wdrożyć i utrzymywać procesy służące identyfikacji miejsc Przetwarzania Wrażliwych Danych Osobowych oraz zapewnić Przetwarzanie Wrażliwych Danych Osobowych wyłącznie, gdy:

- Przetwarzanie Danych jest niezbędne:
  - Dla Administratora Danych lub Osoby Fizycznej w celu wykonania lub skorzystania ze szczególnych praw na mocy odpowiedniego stosunku pracy i ubezpieczenia społecznego oraz prawa do ochrony socjalnej w stopniu, w jakim zezwalają na to stosowne przepisy i regulacje obowiązujące w EOG;
  - W celu ochrony żywotnych interesów Osoby Fizycznej lub innej osoby fizycznej w przypadkach gdy Osoba Fizyczna jest fizycznie lub prawnie niezdolna do udzielenia zgody;
  - W celu ustalenia, realizacji lub obrony roszczeń prawnych lub w każdym przypadku działania przez sądy w ramach ich jurysdykcji;
  - Na potrzeby medycyny prewencyjnej lub medycyny pracy, oceny zdolności Pracownika do pracy, diagnostyki medycznej, opieki zdrowotnej lub społecznej lub leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub społecznej na mocy stosownych przepisów i regulacji obowiązujących w EOG lub na mocy umowy z pracownikiem służby zdrowia objętym obowiązkiem zachowania tajemnicy zawodowej lub w przypadku innej osoby również objętej równoważnym obowiązkiem zachowania tajemnicy;
  - W interesie publicznym w dziedzinie zdrowia publicznego, np. ochrony przed poważnymi transgranicznymi zagrożeniami zdrowia lub zapewnienia wysokich standardów jakości i bezpieczeństwa służby zdrowia i produktów leczniczych czy wyrobów medycznych na podstawie stosownych przepisów i regulacji obowiązujących w EOG, przewidujących odpowiednie i szczególne środki zabezpieczenia praw i wolności Osoby Fizycznej, szczególnie zachowanie tajemnicy zawodowej;
  - W związku z ważnym interesem publicznym na mocy stosownych przepisów i regulacji obowiązujących w EOG, który to interes musi być proporcjonalny do wyznaczonego celu, wyrażać poszanowanie dla istoty prawa do prywatności i ochrony danych oraz przewidywać odpowiednie i szczególne środki zabezpieczenia podstawowych praw i interesów Osoby Fizycznej; lub
  - W celu dokonania archiwizacji w interesie publicznym, na potrzeby badań naukowych lub historycznych lub w celach statystycznych, zgodnie ze stosownymi przepisami i regulacjami obowiązującymi w EOG, które to cele muszą być proporcjonalne do wyznaczonego celu, wyrażać poszanowanie dla istoty prawa do prywatności i ochrony danych oraz przewidywać odpowiednie i szczególne środki zabezpieczenia podstawowych praw i interesów Osoby Fizycznej;
- Przetwarzanie Danych dotyczy Wrażliwych Danych Osobowych wyraźnie udostępnionych publicznie przez Osobę Fizyczną; lub
- Osoba Fizyczna udzieliła zgody na Przetwarzanie Danych w jednym lub większej liczbie określonych celów z wyjątkiem sytuacji, gdy zabraniają tego stosowne przepisy i regulacje obowiązujące w EOG.

4. Legalność przetwarzania danych o wyrokach skazujących i przestępstwach w przypadku przetwarzania danych w EOG i przekazywania danych zgodnie z WRK

Podmioty OE działające jako Administratorzy Danych nie mogą przetwarzać Danych Osobowych dotyczących wyroków skazujących i przestępstw lub powiązanych z nimi środków bezpieczeństwa inaczej niż pod kontrolą organu władzy publicznej lub gdy Przetwarzanie Danych jest dozwolone stosownymi przepisami i regulacjami obowiązującymi w EOG i przewidującymi odpowiednie zabezpieczenie praw i wolności Osób Fizycznych.

V. Stosunki z podmiotami przetwarzającymi dane

1. Globalne wymogi minimalne

Dane Osobowe mogą być gromadzone wyłącznie przez Podmioty Przetwarzające Dane w imieniu Podmiotów OE działających jako Administratorzy Danych na podstawie pisemnej umowy.

2. Wymogi dodatkowe wobec przetwarzania danych w EOG i przekazywania danych zgodnie z WRK

Podmioty OE działające jako Administratorzy Danych muszą:

- Sprawdzać należytą staranność i dokonywać ocen ryzyka w celu ewaluacji Podmiotów Przetwarzających Dane, aby zapewnić, że takie Podmioty Przetwarzające Dane mogą udzielić wystarczających gwarancji co do środków technicznych i organizacyjnych regulujących przewidywane Przetwarzanie Danych sprawiających, że Przetwarzanie Danych będzie spełniać wymogi bezpieczeństwa i poufności określone w Rozdziale B, Dział VII ust. 2:
- Zawrzeć pisemną umowę z preferowanym Podmiotem Przetwarzającym Dane zawierającą wymogi minimalne określone w Załączniku C (Wymogi minimalne odnośnie umów zawieranych między administratorem danych a podmiotem przetwarzającym dane o przetwarzaniu danych w EOG i przekazywaniu danych zgodnie z WRK); oraz
- Okresowo monitorować Podmioty Przetwarzające Dane w celu zweryfikowania bieżącego przestrzegania ich zobowiązań umownych i obowiązków dotyczących zachowania zgodności.

VI. Przekazywanie danych i dalsze przekazywanie danych

1. Globalne wymagania minimalne

Podmioty OE mogą ujawniać, wymieniać lub przekazywać Dane Osobowe innym Podmiotom OE lub Administratorom Danych lub Podmiotom Przetwarzającym Dane niebędącym członkami Grupy Allianz wyłącznie zgodnie z niniejszym SOPA i na podstawie pisemnych umów, chyba że stosowne przepisy i regulacje wyraźnie zezwalają na taką wymianę lub przekazanie danych.

Podmioty OE mogą ujawniać, wymieniać lub przekazywać Dane Osobowe dla celów innych niż określony cel biznesowy Administratorom Danych lub Podmiotom Przetwarzającym Dane niebędącym członkami Grupy Allianz wyłącznie, jeżeli zezwalają na to stosowne przepisy i regulacje lub w razie uzyskania wyraźnej zgody Osoby Fizycznej.

2. Wymogi dodatkowe wobec przetwarzania danych w EOG i przekazywania danych zgodnie z WRK

Podmioty OE mogą przekazywać Dane Osobowe Podmiotom OE spoza EOG (działającym albo jako Administratorzy Danych albo jako Podmioty Przetwarzające Dane), które przestrzegają Wymogów wobec przekazywania danych zgodnie z WRK i które są stroną Umowy Międzyzakładowej.

Przekazywanie Danych Osobowych Podmiotom OE spoza EOG, które nie są stroną Umowy Międzyzakładowej, lub przekazywanie Danych Osobowych przez Podmioty OE z EOG na rzecz Administratorów Danych lub Podmiotów Przetwarzających Dane spoza EOG niebędących członkami Grupy Allianz, lub dalsze przekazywanie Danych Osobowych przez Podmioty OE spoza EOG na rzecz Administratorów Danych lub Podmiotów Przetwarzających Dane niebędących członkami Grupy Allianz, jest dozwolone na podstawie:

- Odpowiedniej decyzji wydanej przez Komisję Europejską: lub
- Zapewnienia przez Administratora Danych lub Podmiot Przetwarzający Dane odpowiednich zabezpieczeń odnośnie przekazywanych Danych Osobowych (np. w drodze standardowych klauzul ochrony danych przyjętych przez Komisję Europejską lub organ ochrony danych działający na terenie EOG) zgodnie z art. 26 Dyrektywy 95/46M/E, który z dniem 25 maja 2018 roku zostanie zastąpiony przez art. 46 Rozporządzenia RODO; lub
- W szczególnych, ograniczonych przypadkach dozwolonych przez stosowne przepisy i regulacje obowiązujące w EOG (np. wyraźna i świadoma zgoda Osoby Fizycznej na przekazanie danych; konieczność dokonania przekazania danych na potrzeby realizacji umowy zawartej między Osobą Fizyczną a Administratorem Danych) - zgodnie z art. 26 ust (1) Dyrektywy 95/46/WE, który z dniem 25 maja 2018 roku zostanie zastąpiony przez art. 49 Rozporządzenia RODO; lub
- Od dnia 25 maja 2018 roku i w ostateczności - w przypadku gdy przekazanie danych jest niezbędne na potrzeby istotnych uzasadnionych interesów Administratora Danych pod warunkiem, że:
  - Przekazywanie danych nie powtarza się i dotyczy wyłącznie ograniczonej liczby Osób Fizycznych;
  - Interes lub prawa i wolności Osoby Fizycznej nie mają nadrzędnego charakteru wobec uzasadnionych interesów Administratora Danych;
  - Administrator Danych oceni wszelkie okoliczności towarzyszące przekazaniu danych i, na podstawie takiej udokumentowanej oceny, zapewni odpowiednie zabezpieczenia odnośnie prywatności i ochrony danych; oraz
  - Administrator Danych poinformuje organ ochrony danych działający na terenie EOG oraz Osobę Fizyczną o przekazaniu danych i o istotnych uzasadnionych interesach.

VII. Bezpieczeństwo i poufność danych

1. Globalne wymogi minimalne

Podmioty OE są zobowiązane do traktowania Danych Osobowych zgodnie ze Standardem bezpieczeństwa informacji w Allianz.

2. Wymogi dodatkowe wobec przetwarzania danych w EOG i przekazywania danych zgodnie z WRK

Podmioty OE muszą przyjąć środki zabezpieczające przed ryzykiem wynikającym z Przetwarzania Danych Osobowych, szczególnie przed utratą, przypadkowym lub bezprawnym zniszczeniem, zmianą, nieuprawnionym ujawnieniem lub dostępem do przekazywanych, przechowywanych lub w inny sposób przetwarzanych Danych Osobowych.

Biorąc pod uwagę obecny stan wiedzy, koszty wdrożenia, charakter, zakres, kontekst i cele Przetwarzania Danych oraz dotkliwość i prawdopodobieństwo zagrożeń dla praw i wolności Osób Fizycznych, Podmioty OE muszą wdrożyć następujące odpowiednie środki techniczne i organizacyjne zapewniające poziom bezpieczeństwa odpowiadający zagrożeniu:

- Anonimizacja Danych Osobowych;
- Pseudonimizacja i zaszyfrowanie Danych Osobowych;
- Zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporność systemów i usług Przetwarzania Danych;
- Zdolność do bezzwłocznego przywrócenia dostępności Danych Osobowych

i dostęp do nich w razie incydentu fizycznego lub technicznego:

- Procesy regularnego testowania, oceniania i szacowania skuteczności środków technicznych i organizacyjnych zapewniających bezpieczeństwo Przetwarzania Danych;
- Procesy zapewniające, że jakakolwiek osoba fizyczna działająca z upoważnienia Administratora Danych lub Podmiotu Przetwarzającego Dane i mająca dostęp do Danych Osobowych będzie Przetwarzać Dane Osobowe tylko na polecenie Administratora Danych lub gdy wymagają tego stosowne przepisy i regulacje obowiązujące w EOG; lub
- Ciągłość działania oraz plany przywrócenia gotowości do pracy i plany awaryjne.

VIII. Utrata danych osobowych

1. Globalne wymogi minimalne

Podmioty OE muszą wdrożyć i utrzymywać skuteczne procesy zapewniające terminowe powiadamianie Specjalisty ds. Prywatności Danych/Inspektora Ochrony Danych Podmiotu OE w razie incydentu utraty lub wycieku danych, który obejmuje lub może obejmować Dane Osobowe („Utrata Danych Osobowych").

Dalsze wymogi zostały określone w Dyrektywach bezpieczeństwa informacji w Allianz i innych politykach i standardach obowiązujących w Allianz i przekazywanych Podmiotom OE.

2. Wymogi dodatkowe wobec przetwarzania danych w EOG i przekazywania danych zgodnie z WRK

Podmioty OE muszą wdrożyć i utrzymywać procesy dokonywania oceny stosownych obowiązków dotyczących dokonywania zgłoszeń odnośnie prywatności i ochrony danych, w tym powiadamiania właściwych organów ochrony danych działających na terenie EOG i Osób Fizycznych.

2.1. Powiadamianie właściwego organu ochrony danych działającego na terenie EOG:

Podmioty OE działające jako Administratorzy Danych muszą, bez zbędnej zwłoki i tam, gdzie jest to możliwe, nie później niż w ciągu 72 godzin od powzięcia wiedzy o incydencie Utraty Danych Osobowych, który może skutkować zagrożeniem dla praw i wolności Osoby Fizycznej, udokumentować i zgłosić incydent Utraty Danych Osobowych do właściwego organu ochrony danych działającego na terenie EOG i podać mu:

- Charakter incydentu Utraty Danych Osobowych, w tym, tam, gdzie to możliwe, kategorie i przybliżoną liczbę Osób Fizycznych, których to dotyczy, oraz kategorie i przybliżoną liczbę zapisów Danych Osobowych, których to dotyczy;
- Imię i nazwisko oraz dane kontaktowe Specjalisty ds. Prywatności Danych/ Inspektora Ochrony Danych Podmiotu OE lub innego punktu kontaktowego, który może udzielić dalszych informacji;
- Możliwe konsekwencje incydentu Utraty Danych Osobowych; oraz
- Środki podjęte lub proponowane do podjęcia przez Podmiot OE w celu zareagowania na incydent Utraty Danych Osobowych obejmujące, w stosownych przypadkach, środki łagodzące możliwe negatywne skutki takiego incydentu.

Jeżeli takie informacje nie mogą być przekazane jednocześnie, mogą zostać podane etapami bez dalszej zbędnej zwłoki.

2.2. Powiadamianie osób fizycznych

Podmioty OE działające jako Administratorzy Danych muszą, bez zbędnej zwłoki, informować Osobę Fizyczną, której to dotyczy, o incydencie Utraty Danych Osobowych, jeśli taki incydent może skutkować wysokim poziomem zagrożenia dla praw i wolności Osoby Fizycznej, i w takim powiadomieniu w jasnym i prostym języku opiszą:

- Charakter incydentu Utraty Danych Osobowych;
- Imię i nazwisko oraz dane kontaktowe Specjalisty ds. Prywatności Danych/Inspektora Ochrony Danych Podmiotu OE lub innego punktu kontaktowego, który może udzielić dalszych informacji;
- Możliwe konsekwencje incydentu Utraty Danych Osobowych; oraz
- Środki podjęte lub proponowane do podjęcia przez Podmiot OE w celu zareagowania na incydent Utraty Danych Osobowych obejmujące, w stosownych przypadkach, środki łagodzące możliwe negatywne skutki takiego incydentu.

Podmioty OE działające jako Administratorzy Danych nie muszą przekazać powiadomienia, jeżeli:

- Podmiot OE wdrożył odpowiednie techniczne i organizacyjne środki ochronne i środki te zastosowano wobec Danych Osobowych objętych incydentem Utraty Danych Osobowych, a szczególnie środki sprawiające, że Dane Osobowe stają się nieczytelne dla każdego, kto nie jest uprawniony do dostępu do nich (np. szyfrowanie);
- Podmiot OE podjął dalsze środki zapewniające, że wystąpienie wysokiego poziomu zagrożenia dla praw i wolności Osoby Fizycznej jest mało prawdopodobne; lub
- Wiązałoby się to z niewspółmiernym wysiłkiem, w którym to przypadku Podmiot OE musi wydać publiczny komunikat lub zastosować podobny środek, za pomocą którego w równie skuteczny sposób poinformuje Osoby Fizyczne, których to dotyczy.

2.3. Powiadamianie Administratora Danych

Podmioty OE działające jako Podmioty Przetwarzające Dane muszą, bez zbędnej zwłoki po powzięciu wiedzy o incydencie Utraty Danych Osobowych, powiadomić o tym Administratora Danych.

IX. Ochrona prywatności w fazie projektowania i domyślna ochrona prywatności

1. Ochrona prywatności w fazie projektowania

1.1. Globalne wymogi minimalne

Podmioty OE muszą zapewnić metodyczne włączenie prywatności i ochrony danych we właściwe procesy i procedury biznesowe oraz w systemy informatyczne i aplikacje, których to dotyczy.

1.2. Wymogi dodatkowe wobec przetwarzania danych w EOG i przekazywania danych zgodnie z WRK

Podmioty OE działające jako Administratorzy Danych są zobowiązane do wdrożenia odpowiednich środków technicznych i organizacyjnych (np. pseudonimizacji) skutecznie wdrażających zasady dotyczące prywatności i ochrony danych (np. minimalizacja danych) w nowych produktach, usługach i procesach i procedurach biznesowych, w stosownych przypadkach, oraz włączających niezbędne

zabezpieczenia w Przetwarzanie Danych Osobowych.

Podmioty OE muszą wdrożyć takie środki zarówno w czasie ustalania sposobów Przetwarzania Danych, jak i w trakcie samego Przetwarzania Danych.

Podmioty OE muszą uwzględnić stan wiedzy, koszty wdrożenia oraz charakter, zakres, kontekst i cele Przetwarzania Danych, a także dotkliwość i prawdopodobieństwo zagrożeń dla praw i wolności Osób Fizycznych spowodowanych Przetwarzaniem Danych.

2. Ochrona prywatności w fazie projektowania

Podmioty OE działające jako Administratorzy Danych muszą wdrożyć odpowiednie środki techniczne i organizacyjne w celu zapewnienia, że domyślnie przetwarzane będą wyłącznie Dane Osobowe niezbędne dla każdego określonego celu Przetwarzania Danych. Wymóg ten ma zastosowanie do ilości zgromadzonych Danych Osobowych, stopnia Przetwarzania Danych, okresu ich przechowywania i dostępu do danych. W szczególności, Dane Osobowe nie mogą być domyślnie dostępne dla nieograniczonej liczby osób fizycznych bez ingerencji Osoby Fizycznej (np. informacje zwrotne lub komentarze przekazane przez Internet nie powinny być domyślnie upubliczniane).

X. Współpraca z właściwymi organami ochrony danych działającymi na terenie EOG w zakresie przetwarzania danych w EOG i przekazywania danych zgodnie z WRK

Podmioty OE muszą współpracować z organami ochrony danych działającymi na terenie EOG w zakresie wykonywanych przez nie obowiązków i stosować się do ich rad odnośnie wszelkich kwestii w zakresie Wymogów dotyczących przekazywania danych zgodnie z WRK.

C. Zasady przestrzegania prywatności i ochrony danych

Poniższe czynności i procesy dotyczące przestrzegania prywatności i ochrony danych zostały opracowane w celu umożliwienia przestrzegania zasad określonych w Rozdziale B i udzielenia Podmiotowi OE wsparcia przy wypełnianiu zobowiązań wobec Osób Fizycznych przedstawionych w Rozdziale D.

I. Dokumentacja operacji przetwarzania danych

Podmioty OE muszą ustanowić i utrzymywać pisemną ewidencję obejmującą wszystkie wykonywane przez siebie operacje Przetwarzania Danych. Dalsze wymogi zostały opisane w odpowiedniej *Zasadzie funkcjonalnej dokumentowania operacji przetwarzania danych.*

II. Szkolenia

1. Globalne wymogi minimalne

Podmioty OE muszą ustanowić i przeprowadzać okresowe szkolenia z dziedziny prywatności i ochrony danych dla Pracowników w celu zapewnienia odpowiedniego poziomu ich wiedzy i świadomości.

2. Wymogi dodatkowe wobec przekazywania danych zgodnie z WRK

Podmioty OE muszą zapewnić Pracownikom stale lub regularnie zaangażowanym w Przetwarzanie Danych lub opracowywanie narzędzi używanych do Przetwarzania Danych Osobowych w EOG odpowiednie szkolenia z dziedziny prywatności i ochrony danych obejmujące szkolenia dotyczące Wymogów w zakresie przetwarzania danych w EOG i Wymogów w zakresie przekazywania danych zgodnie z WRK.

Podmioty OE mogą skorzystać ze szkolenia z wykorzystaniem komputera, z corocznym przypomnieniem wiedzy, które, dla Grupy Allianz, przygotowuje i realizuje Allianz SE. W ramach szkolenia zostanie sprawdzony poziom znajomości wiedzy przekazanej Pracownikom. W zakresie dozwolonym przez stosowne przepisy i regulacje podmioty OE muszą monitorować poziom i wyniki ukończonych testów.

III. Wewnętrzny mechanizm rozpatrywania skarg

1. Globalne wymogi minimalne

Podmioty OE są zobowiązane do wdrożenia i utrzymywania skutecznych procesów zajmujących się kwestią prywatności i ochrony danych w odniesieniu do skarg, zapytań i incydentów.

2. Wymogi dodatkowe wobec przekazywania danych zgodnie z WRK

W przypadku skarg złożonych przez Osoby Fizyczne i dotyczących Przekazywania Dany zgodnie z WRK Podmioty OE muszą przestrzegać procedury określonej w Załączniku D Dział II. (Rozpatrywanie wniosków osób fizycznych dotyczących przetwarzania danych w EOG oraz skarg dotyczących przekazywania danych zgodnie z WRK).

IV. Oceny wpływu na prywatność

Podmioty OE działające jako Administratorzy Danych muszą, za pomocą Oceny Wpływu na Prywatność, ocenić legalność i wpływ Przetwarzania Danych Osobowych na wszystkie procesy i procedury stanowiące zagrożenie od średniego do wysokiego stopnia dla prywatności i ochrony danych przed ich wdrożeniem.

Specjalista ds. Prywatności Danych/Inspektor Ochrony Danych Podmiotu OE może, w oparciu o swój profesjonalny osąd, doradzić przeprowadzenie Oceny Wpływu na Prywatność w stosunku do procesów wywołujących niski stopień zagrożenia dla prywatności i ochrony danych (np. typowe procesy biurowe).

Dalsze wymogi dotyczące Ocen Wpływu na Prywatność określono w *Zasadzie funkcjonalnej prowadzenia i dokumentowania ocen wplywu na prywatność*.

V. Monitorowanie i zapewnienie zgodności

1. Globalne wymogi minimalne

Podmioty OE, globalne linie i regiony muszą prowadzić oparty na ryzyku nadzór (który może obejmować monitoring, testowanie i inne elementy) nad odpowiednim projektem, wdrożeniem i skutecznością Ram i powiązanych z nimi procesów i kontroli. Podmioty OE muszą, przez okres 5 lat, poddawać Ramy testom obejmującym próbki, ankiety i przeglądy.

Wyniki muszą zostać terminowo zatwierdzone przez Zarząd Podmiotu OE i przekazane Dyrektorowi Grupy ds. Prywatności (lub jego Specjaliście ds. Prywatności Danych/Inspektorowi Ochrony Danych w regionie lub globalnej linii).

Podmioty OE muszą przedstawić sprawozdanie ze zgodności z Ramami, gdy wymaga tego Dyrektor Grupy ds. Prywatności.

2. Wymogi dodatkowe wobec przekazywania danych zgodnie z WRK

Podmioty OE muszą regularnie lub na konkretną prośbę Dyrektora Grupy ds. Prywatności albo innego Podmiotu OE brać udział w audytach z zakresu prywatności i ochrony danych (przynajmniej co 5 lat).

Takie audyty muszą być przeprowadzane przez akredytowanych profesjonalistów (wewnętrznych lub zewnętrznych) i muszą obejmować Wymogi wobec przekazywania danych zgodnie z WRK, w tym metody zapewniające skuteczną kontynuację i wdrażanie działań naprawczych.

Wyniki audytu muszą zostać przekazane Specjaliście ds. Prywatności Danych/Inspektorowi Ochrony Danych Podmiotu OE, Zarządowi Podmiotu OE, Dyrektorowi Grupy ds. Prywatności, Zarządowi Allianz SE oraz, na wniosek, dowolnemu organowi ochrony danych, działającemu na terenie EOG.

Podmiot OE może być poddany audytowi przeprowadzanemu przez organ ochrony danych działający na terenie EOG i musi bezzwłocznie poinformować Specjalistę ds. Prywatności Danych/Inspektora Ochrony Danych Podmiotu OE i Dyrektora Grupy ds. Prywatności (i Specjalisty ds. Prywatności Danych/Inspektora Ochrony Danych Podmiotu OE w regionie lub globalnej linii), jeżeli jakikolwiek organ ochrony danych działający na terenie EOG zażąda przedstawienia wyników audytu lub ma zamiar przeprowadzić audyt z zakresu prywatności i ochrony danych.

D. Obowiązki wobec osób fizycznych

I. Udzielanie odpowiedzi na wnioski osób fizycznych o uzyskanie dostępu, sprostowanie lub usunięcie danych

1. Globalne wymogi formalne

Podmioty OE działające jako Administratorzy Danych muszą zapewnić Osobom Fizycznym możliwość przeglądu, sprostowania lub usunięcia swoich Danych Osobowych na wniosek i zgodnie ze stosownymi przepisami i regulacjami, jeżeli Osoby Fizyczne najpierw uwierzytelnią w odpowiednim stopniu swoją tożsamość.

Jeżeli Podmiot OE odrzuci taki wniosek, musi podać Osobom Fizycznym powody takiej odmowy oraz zapewnić im możliwość zakwestionowania takiej decyzji.

2. Wymogi dodatkowe wobec przetwarzania danych w EOG i przekazywania danych zgodnie z WRK

Odpowiadając na wnioski Osób Fizycznych o uzyskanie dostępu, sprostowanie lub usunięcie danych, Podmioty OE muszą przestrzegać procedury określonej w Załączniku D, Dział I. (Rozpatrywanie wniosków osób fizycznych dotyczących przetwarzania danych w EOG oraz skarg dotyczących przekazywania danych zgodnie z WRK).

2.1. Wniosek o uzyskanie dostępu do danych

Podmioty OE działające jako Administratorzy Danych muszą zapewnić Osobom Fizycznym możliwość uzyskania, na wniosek, dostępu do poniższych informacji:

- Potwierdzenia, czy Administrator Danych posiada dotyczące ich Dane Osobowe;
- Kopii swoich Danych Osobowych;
- Celu(-ów) Przetwarzania Danych;
- Kategorii przechowywanych Danych Osobowych o Osobie Fizycznej;
- Odbiorców lub kategorii odbiorców, którym ujawniane są Dane Osobowe (szczególnie odbiorców w krajach spoza EOG) oraz odpowiednich zabezpieczeń stosowanych przy takim przekazywaniu danych;
- Tam, gdzie to możliwe, okresu przechowywania Danych Osobowych lub, jeśli nie jest to możliwe, kryteriów stosowanych w celu ustalenia tego okresu;
- Istnienia prawa do wnioskowania do Administratora Danych o sprostowanie lub usunięcie Danych Osobowych lub ograniczenie Przetwarzania Danych Osobowych dotyczących Osoby Fizycznej lub do wniesienia sprzeciwu wobec takiego Przetwarzania Danych;
- Prawa do złożenia skargi do organu ochrony danych działającego na terenie EOG;
- W przypadkach gdy Dane Osobowe nie są zbierane od Osoby Fizycznej - wszelkich dostępnych informacji odnośnie źródła; oraz
- Istnienia zautomatyzowanego procesu podejmowania decyzji obejmującego Profilowanie, o którym mowa w Rozdziale D, Dział V, oraz, przynajmniej w takich przypadkach, istotnych informacji dotyczących zastosowanej logiki oraz znaczenia i przewidywanych konsekwencji takiego Przetwarzania Danych dla Osoby Fizycznej.

Podmioty OE działające jako Administratorzy Danych mogą odrzucić takie wnioski w przypadkach wymienionych w Załączniku D, Dział I. ust. 5 (Rozpatrywanie wniosków osób fizycznych, dotyczących przetwarzania danych w EOG oraz skarg dotyczących przekazywania danych zgodnie z WRK).

2.2. Wniosek o sprostowanie danych

Podmioty OE działające jako Administratorzy Danych muszą zapewnić Osobom Fizycznym możliwość wnioskowania, bez zbędnej zwłoki, o sprostowanie Danych Osobowych niezgodnych ze stosownymi przepisami i regulacjami obowiązującymi w EOG, w szczególności z powodu ich niekompletności lub niedokładności, w tym w drodze przedstawienia dodatkowego oświadczenia uwzględniającego cel(-e) Przetwarzania Danych.

Podmioty OE działające jako Administratorzy Danych mogą odrzucić takie wnioski w przypadkach wymienionych w Załączniku D, Dział I, ust. 5 (Rozpatrywanie wniosków osób fizycznych dotyczących przetwarzania danych w EOG oraz skarg dotyczących przekazywania danych zgodnie z WRK).

2.3. Wniosek o usunięcie danych

Podmioty OE działające jako Administratorzy Danych muszą zapewnić Osobom Fizycznym możliwość wnioskowania o usunięcie swoich Danych Osobowych, jeżeli:

- Dane Osobowe nie są już niezbędne w odniesieniu do celu(-ów), do jakich zostały one zgromadzone lub w inny sposób Przetworzone;
- Osoba Fizyczna cofnie zgodę, na której opiera się Przetwarzanie Danych, i nie istnieje żadna inna podstawa prawna dla Przetwarzania Danych;
- Osoba Fizyczna zgłosi sprzeciw wobec Przetwarzania Danych prowadzonego na podstawie uzasadnionych interesów Administratora Danych, gdy nie istnieją żadne nadrzędne, uzasadnione podstawy Przetwarzania Danych lub gdy Osoba Fizyczna wniesie sprzeciw wobec Przetwarzania Danych prowadzonego w celach marketingu bezpośredniego;
- Dane Osobowe zostały przetworzone bezprawnie;
- Dane Osobowe muszą zostać usunięte na potrzeby przestrzegania stosownych przepisów i regulacji obowiązujących w EOG, którym podlega Administrator Danych, lub;
- Dane Osobowe dotyczą dziecka lub Osoby Fizycznej, której Dane Osobowe zostały zgromadzone, gdy taka osoba była dzieckiem, jak określono w stosownych przepisach i regulacjach obowiązujących w EOG, i zostały zgromadzone w odniesieniu do oferty usług społeczeństwa informacyjnego.

W przypadkach gdy Dane Osobowe podlegające wnioskowi o usunięcie zostały upublicznione przez Administratora Danych Administrator Danych musi podjąć uzasadnione środki, obejmujące środki techniczne, w celu poinformowania Administratorów Danych Przetwarzających Dane Osobowe o wniosku Osoby Fizycznej o usunięcie wszelkich odnośników do takich Danych Osobowych lub ich kopii.

Podmioty OE działające jako Administratorzy Danych mogą odrzucić wniosek Osoby Fizycznej o usunięcie swoich Danych Osobowych w przypadkach wymienionych w Załączniku D, Dział I, ust. 5 (Rozpatrywanie wniosków osób fizycznych dotyczących przetwarzania danych w EOG oraz skarg dotyczących przekazywania danych zgodnie z WRK). W takim przypadku Podmioty OE mogą ograniczyć Przetwarzanie Danych Osobowych podlegających wnioskowi o usunięcie w razie złożenia przez Osobę Fizyczną dalszego wniosku zgodnie z Rozdziałem D, Dział III.

II. Udzielanie odpowiedzi na wnioski osób fizycznych dotyczące sprzeciwu wobec przetwarzania danych w EOG i przekazywania danych zgodnie z WRK

Podmioty OE działające jako Administratorzy Danych muszą zapewnić Osobom Fizycznym możliwość zgłoszenia, w każdym czasie, sprzeciwu wobec Przetwarzania

ich Danych Osobowych opierającego się na uzasadnionych interesach Administratora Danych, w tym wobec Profilowania. W takim przypadku Podmioty OE muszą zaprzestać Przetwarzania Danych Osobowych, chyba że są w stanie wykazać istotne uzasadnione podstawy dla kontynuacji Przetwarzania Danych, które mają charakter nadrzędny wobec interesów, praw i wolności Osoby Fizycznej, lub istotne uzasadnione podstawy dla ustalenia, realizacji lub obrony roszczeń prawnych.

Podmioty OE działające jako Administratorzy Danych muszą także zapewnić Osobom Fizycznym możliwość zgłoszenia, w każdym czasie, sprzeciwu wobec Przetwarzania ich Danych Osobowych dla celów marketingu bezpośredniego (w tym Profilowania, w stopniu, w jakim odnosi się ono do marketingu bezpośredniego). W takim przypadku Podmioty OE zaprzestaną Przetwarzania Danych dla celów marketingu bezpośredniego.

Odpowiadając na sprzeciw zgłaszany przez Osobę Fizyczną, Podmiot OE musi przestrzegać procedury określonej w Załączniku D, Dział I. (Rozpatrywanie wniosków osób fizycznych dotyczących przetwarzania danych w EOG oraz skarg dotyczących przekazywania danych zgodnie z WRK). Podmioty OE mogą odrzucić takie wnioski w przypadkach wymienionych w Załączniku D, Dział I. ust. 5.

III. Udzielanie odpowiedzi na wnioski osób fizycznych o ograniczenie przetwarzania danych w EOG i przekazywania danych zgodnie z WRK

Z dniem 25 maja 2018 roku Podmioty OE działające jako Administratorzy Danych muszą zapewnić Osobom Fizycznym możliwość ograniczenia Przetwarzania ich Danych Osobowych oraz ich odpowiedniego pogrupowania, jeżeli:

- Dokładność Danych Osobowych zostanie zakwestionowana przez Osoby Fizyczne - przez okres umożliwiający Administratorowi Danych weryfikację dokładności Danych Osobowych;
- Przetwarzanie Danych jest bezprawne, a Osoby Fizyczne sprzeciwią się usunięciu Danych Osobowych i w zamian złożą wniosek o ograniczenie ich wykorzystania;
- Administrator Danych już nie potrzebuje Danych Osobowych dla celów Przetwarzania Danych, ale wymagają ich Osoby Fizyczne na potrzeby ustalenia, realizacji lub obrony roszczeń prawnych; lub
- Osoby Fizyczne zgłosiły sprzeciw wobec Przetwarzania Danych prowadzonego w na podstawie uzasadnionych interesów Administratora Danych - w oczekiwaniu na weryfikację nadrzędnego charakteru uzasadnionych podstaw Administratora Danych w stosunku do podstaw Osób Fizycznych.

W przypadkach gdy Przetwarzanie Danych jest ograniczone Podmioty OE mogą, z wyjątkiem przechowywania, Przetwarzać Dane Osobowe wyłącznie:

- Za zgodą Osoby Fizycznej;
- Na potrzeby ustalenia, realizacji lub obrony roszczeń prawnych;
- W celu ochrony praw innej osoby fizycznej lub prawnej; lub
- Z uwagi na ważny interes publiczny określony w stosownych przepisach i regulacja obowiązujących w EOG.

Jeżeli Podmioty OE działające jako Administratorzy Danych w większym stopniu ograniczą Przetwarzanie Danych na wniosek Osoby Fizycznej, muszą poinformować Osobę Fizyczną o takim ograniczenia Przetwarzania Danych przed jego zniesieniem.

Odpowiadając na wnioski Osób Fizycznych o ograniczenie Przetwarzania Danych, Podmioty OE muszą przestrzegać procedury określonej w Załączniku D, Dział I. (Rozpatrywanie wniosków osób fizycznych dotyczących przetwarzania danych w

EOG oraz skarg dotyczących przekazywania danych zgodnie z WRK). Podmioty OE mogą odrzucić takie wnioski w przypadkach wymienionych w Załączniku D, Dział I. ust. 5.

IV. Udzielanie odpowiedzi na wnioski osób fizycznych o umożliwienie przenoszalności danych odnośnie przetwarzania danych w EOG i przekazywania danych zgodnie z WRK

Z dniem 25 maja 2018 roku, w przypadkach gdy Przetwarzanie Danych opiera się na zgodzie lub umowie i jest przeprowadzane w sposób zautomatyzowany, Podmioty OE działające jako Administratorzy Danych muszą zapewnić Osobom Fizycznym możliwość wnioskowania o:

- Otrzymanie Danych Osobowych przekazanych Podmiotowi OE działającemu jako Administrator Danych w ustrukturyzowanym, powszechnie używanym i nadającym się do przetwarzania maszynowego formacie; oraz
- Przekazanie Danych Osobowych innemu Administratorowi Danych bez przeszkód ze strony pierwotnego Administratora Danych lub ich bezpośrednie przekazanie przez jednego do drugiego Administratora Danych, tam, gdzie jest to technicznie wykonalne.

Wniosek Osoby Fizycznej o przeniesienie swoich Danych Osobowych pozostaje bez uszczerbku dla prawa Osoby Fizycznej do wnioskowania o usunięcie danych i nie ma on negatywnego wpływu na prawa i wolności innych osób.

Odpowiadając na wnioski Osób Fizycznych o przeniesienie danych, Podmioty OE muszą przestrzegać procedury określonej w Załączniku D, Dział I. (Rozpatrywanie wniosków osób fizycznych dotyczących przetwarzania danych w EOG oraz skarg dotyczących przekazywania danych zgodnie z WRK). Podmioty OE mogą odrzucić takie wnioski w przypadkach wymienionych w Załączniku D, Dział I. ust. 5.

V. Udzielanie odpowiedzi na wnioski osób fizycznych dotyczące sprzeciwu wobec zautomatyzowanych decyzji w sprawie przetwarzania danych w EOG i przekazywania danych zgodnie z WRK

Podmioty OE działające jako Administratorzy Danych muszą zapewnić Osobom Fizycznym możliwość zgłoszenia sprzeciwu wobec jakiejkolwiek decyzji wywołującej skutek prawny dotyczący takiej Osoby Fizycznej lub decyzji, która w inny sposób znacząco wpływa na taką Osobę Fizyczną, a która opiera się wyłącznie na zautomatyzowanym Przetwarzaniu Danych Osobowych takiej Osoby Fizycznej, a z dniem 25 maja 2018 roku - decyzji opartej na Profilowaniu.

Podmioty OE mogą odrzucić taki wniosek, jeżeli decyzja:

- Jest niezbędna dla zawarcia lub realizacji umowy zawartej pomiędzy Osobą Fizyczną a Podmiotem OE działającym jako Administrator Danych;
- Jest dozwolona w stosownych przepisach i regulacjach obowiązujących w EOG, którym podlega Podmiot OE działający jako Administrator Danych i które ustanawiają właściwe środki zabezpieczające prawa i wolności oraz uzasadnione interesy Osoby Fizycznej; lub
- Opiera się na wyraźnej zgodzie Osoby Fizycznej.

Podmioty OE działające jako Administratorzy Danych mogą podejmować decyzje oparte jedynie na zautomatyzowanym Przetwarzaniu Wrażliwych Danych Osobowych Osoby Fizycznej, jeżeli wdrożyły właściwe środki zabezpieczające prawa i wolności oraz uzasadnione interesy Osoby Fizycznej, oraz:

- Osoba Fizyczna udzieliła wyraźnej zgody, lub
- Przetwarzanie Danych jest niezbędne z uwagi na ważny interes publiczny na podstawie stosownych przepisów i regulacji obowiązujących w EOG.

Odpowiadając na sprzeciw zgłaszany przez Osobę Fizyczną wobec decyzji dotyczących Osoby Fizycznej opartych na zautomatyzowanym Przetwarzaniu, w tym Profilowaniu, Podmiot OE musi przestrzegać procedury określonej w Załączniku D, Dział 1. (Rozpatrywanie wniosków osób fizycznych dotyczących przetwarzania danych w EOG oraz skarg dotyczących przekazywania danych zgodnie z WRK). Podmioty OE mogą odrzucić takie wnioski w przypadkach wymienionych w Załączniku D, Dział I. ust. 5.

E. Obowiązki wobec osób fizycznych

I. Poziom Grupy Allianz

1. Zarząd Allianz SE

Zarząd Allianz SE ponosi całkowitą odpowiedzialność za przestrzeganie prywatności ochrony danych. Zobowiązany jest uwzględniać niniejszy SOPA.

2. Dział Prywatności i Ochrony Danych Grupy

Całkowita odpowiedzialność za Dział Prywatności i Ochrony Danych Grupy spoczywa na członku Zarządu Allianz SE kierującym działem handlowym H6. Działowi Prywatności i Ochrony Danych Grupy powierzono odpowiedzialność za przestrzeganie ochrony i prywatności danych i do jego obowiązków należy:

- Udzielanie Podmiotom OE porad w zakresie wszelkich kwestii związanych z przestrzeganiem prywatności i ochrony danych oraz wspieranie i prowadzenie współpracy z osobami pełniącymi inne funkcje w powiązanych kwestiach;
- Współpraca z organami władzy, organami regulacyjnymi, stowarzyszeniami i innymi interesariuszami w kwestiach dotyczących prywatności i ochrony danych;
- Monitorowanie przestrzegania przez Podmioty OE niniejszego SOPA, obejmujące:
  - Wdrożenie niniejszego SOPA;
  - Udział w sporządzaniu rocznego sprawozdania w zakresie prywatności i ochrony danych przedkładanego Zarządowi Allianz SE przez Dyrektora Grupy ds. Prywatności, obejmującego informacje o zaawansowaniu prywatności i ochrony danych w obrębie Grupy Allianz oraz wszelkie przypadki istotnej niezgodności z niniejszym SOPA;
  - Przeprowadzanie wszelkich niezbędnych weryfikacji:
  - Utrzymanie i aktualizacja niniejszego SOPA oraz powiadamianie o takich zmianach Podmiotów OE i, na wniosek, Osób Fizycznych;
  - Utrzymanie bazy danych stron Umowy Międzyzakładowej oraz powiadamianie o takich zmianach Podmiotów OE i, na wniosek, Osób Fizycznych;
  - Zgłaszanie wszelkich zmian, obejmujących aktualizacje, dotyczących niniejszego SOPA i stron Umowy Międzyzakładowej, łącznie z corocznym udzielaniem wyjaśnień organom ochrony danych działającym na terenie EOG, a, gdy jest to wymagane, uzyskanie zgody na wprowadzenie jakichkolwiek istotnych zmian w niniejszym SOPA;
- Współpraca ze Specjalistami ds. Prywatności Danych/Inspektorami Ochrony Danych Podmiotów OE oraz Dyrektorem Grupy ds. Prywatności w kwestii odpowiedniej reakcji na incydenty Utraty Danych Osobowych i rozpatrywania Wniosków Podmiotów Danych o Uzyskanie Dostępu.

3. Dział Prywatności i Ochrony Danych Grupy

Dyrektor Grupy ds. Prywatności kieruje GC/Działem Prywatności i Ochrony Danych Grupy w Grupie Allianz. Dyrektora Grupy ds. Prywatności powołuje członek Zarządu Allianz SE kierujący działem handlowym H6.

Dyrektor Grupy ds. Prywatności:

- Bezpośrednio podlega członkowi Zarządu Allianz SE odpowiedzialnemu za dział handlowy H6;
- Właściwie i terminowo angażuje się we wszelkie kwestie dotyczące

prywatności i ochrony danych;

- Posiada odpowiednie zasoby i nieograniczony dostęp do operacji Przetwarzania Danych oraz utrzymuje poziom posiadanej wiedzy fachowej;
- Nie otrzymuje poleceń dotyczących wykonywania swoich zadań;
- Jest objęty ochroną przed zwolnieniem z pracy i karą za wykonywane przez siebie zadania;
- Jest związany zasadą tajemnicy lub poufności odnośnie wykonywanych przez siebie zadań zgodnie ze stosownymi przepisami i regulacjami obowiązującymi w EOG;
- Wykonuje wszelkie inne zadania i obowiązki wyłącznie, gdy nie prowadzą one do konfliktu interesów np. Dyrektor Grupy ds. Prywatności nie może pełnić funkcji, w ramach której ustala cele i sposoby Przetwarzania Danych Osobowych);
- Upubliczni swoje dane kontaktowe i przekaże je głównemu organowi ochrony danych działającemu na terenie EOG do dnia 25 maja 2018 roku oraz powiadomi główny organ ochrony danych działający na terenie EOG o wszelkich zmianach tych danych zaistniałych w późniejszym terminie; oraz
- Jest osiągalny dla Osób Fizycznych we wszelkich kwestiach dotyczących Przetwarzania ich Danych Osobowych i korzystania z ich praw.

Dyrektor Grupy ds. Prywatności odpowiada za skuteczne wdrożenie i utrzymanie prywatności i ochrony danych w całej Grupie Allianz i:

- Udziela porad i szkoli Zarząd Allianz SE w zakresie wszelkich kwestii związanych z przestrzeganiem prywatności i ochrony danych;
- Udziela porad i szkoli Pracowników w zakresie ich praw i obowiązków wynikających z niniejszego SOPA;
- Sporządza, wdraża i monitoruje inicjatywy w dziedzinie prywatności i ochrony danych w całej Grupie;
- Współpracuje z osobami pełniącymi inne funkcje na poziomie Grupy Allianz w zakresie odpowiedniej reakcji na incydenty Utraty Danych Osobowych i Wnioski Podmiotów Danych o Uzyskanie Dostępu;
- Postępuje zgodnie z procedurą rozpatrywania skarg Osób Fizycznych dotyczących Przekazywania Danych zgodnie z WRK określoną w Załączniku D, Dział II. (Rozpatrywanie wniosków osób fizycznych dotyczących przetwarzania danych w EOG oraz skarg dotyczących przekazywania danych zgodnie z WRK) w przypadkach przekazania mu skarg;
- Przedkłada Zarządowi Allianz SE roczne sprawozdanie w zakresie prywatności i ochrony danych obejmujące informacje o zaawansowaniu prywatności i ochrony danych w obrębie Grupy Allianz oraz wszelkie przypadki istotnej niezgodności z niniejszym SOPA;
- Działa jako punkt kontaktowy i współpracuje z organami ochrony danych, działającymi na terenie EOG w zakresie wszelkich wniosków dotyczących Przetwarzania Danych w EOG, w tym uprzednich konsultacji odnośnie Ocen Wpływu na Prywatność czy też Wymogów wobec przekazywania danych zgodnie z WRK;
- Prowadzi w Grupie Allianz sieć Specjalistów ds. Prywatności Danych/Inspektorów Ochrony Danych;
- Organizuje i prowadzi Grupę Doradczą Allianz ds. Prywatności;
- Współpracuje ze Specjalistami ds. Prywatności Danych/Inspektorami Ochrony Danych Podmiotów OE i innymi istotnymi interesariuszami w celu

rozstrzygnięcia każdego konfliktu między postanowieniami niniejszego SOPA a lokalnymi przepisami i regulacjami, aby ustalić odpowiednie działania, a, w przypadku wątpliwości, konsultuje się z organami ochrony danych działającymi na terenie EOG; oraz

- Broni interesów Grupy Allianz w dziedzinie prywatności i ochrony danych w organach władzy, organach regulacyjnych, stowarzyszeniach i u pozostałych interesariuszy.

Dyrektor Grupy ds. Prywatności działa również jako Inspektor Ochrony Danych Podmiotu OE dla Allianz SE i, w tym celu, bezpośrednio podlega członkowi Zarządu Allianz SE odpowiedzialnemu za dział handlowy H6. W tym względzie Dyrektor Grupy ds. Prywatności, wykonując swoje obowiązki, w należyty sposób uwzględnia ryzyko związane z Przetwarzaniem Danych podejmowane przez Allianz SE, mając na uwadze charakter, zakres, kontekst i cel(-e) Przetwarzania Danych.

II. Poziom podmiotów OE Allianz

1. Zarząd Podmiotu OE

1.1. Globalne obowiązki

Dany Zarząd Podmiotu OE odpowiada za ustanowienie i utrzymywanie solidnej i sprecyzowanej struktury organizacyjnej i operacyjnej w celu zapewnienia zgodności z Ramami i:

- Zapewnia odpowiednie zasoby, szkolenia personelu, prowadzenie dokumentacji, jakość danych i systemy informatyczne oraz monitoring;
- Zapewnia zasoby odpowiednie dla przestrzegania procedury rozpatrywania Wniosków Podmiotów Danych o Uzyskanie Dostępu określonej w Załączniku D, Dział 1. (Rozpatrywanie wniosków osób fizycznych dotyczących przetwarzania danych w EOG oraz skarg dotyczących przekazywania danych zgodnie z WRK);
- Gdy wymagają tego stosowne przepisy i regulacje - powołuje wcześniej zaakceptowanego przez Dyrektora Grupy ds. Prywatności Inspektora Ochrony Danych albo na oddzielne stanowisko albo w ramach określonego obowiązku dla istniejącego stanowiska (np. osoby pełniącej w Podmiocie OE funkcje związane z ochroną prawną lub utrzymaniem zgodności), przy czym taki Inspektor Ochrony Danych:
  - Spełnia wymogi zawarte w stosownych przepisach i regulacjach;
  - Posiada kwalifikacje i wiedzę fachową niezbędne dla pełnienia funkcji Inspektora Ochrony Danych, np. odpowiedni poziom rozumienia prowadzonych operacji Przetwarzania Danych, systemów informacyjnych, bezpieczeństwa oraz potrzeb Podmiotu OE w zakresie prywatności i ochrony danych, obejmujących obowiązki określone w Dziale II. poniżej;
  - Podlega członkowi Zarządu Podmiotu OE odpowiedzialnemu za prywatność i ochronę danych; oraz
  - Może działać niezależnie, przy nieograniczonym dostępie do operacji Przetwarzania Danych i informacji oraz nie powodując konfliktu interesów (np. Inspektor Ochrony Danych nie może pełnić funkcji, w ramach której ustala cele i sposoby Przetwarzania Danych Osobowych);
  - Uczestniczy w Grupie Doradczej Allianz ds. Prywatności; oraz
- Gdy powołania Inspektora Ochrony Danych nie wymagają stosowne przepisy i regulacje, powoduje Specjalistę ds. Prywatności Danych i zapewnia mu wsparcie i zasoby odpowiednie dla jego zadań i obowiązków. Taki Specjalista ds. Prywatności Danych:

- Ma kwalifikacje odpowiednie dla jego obowiązków określonych w Dziale 2. poniżej; oraz
- Uczestniczy w Grupie Doradczej Allianz ds. Prywatności, przy czym taka nominacja jest wcześniej akceptowana przez Dyrektora Grupy ds. Prywatności.

1.2. Dodatkowe obowiązki dotyczące przetwarzania danych w EOG i przekazywania danych zgodnie z WRK

Dany Zarząd Podmiotu OE odpowiada za ustanowienie i utrzymywanie solidnej i sprecyzowanej struktury organizacyjnej i operacyjnej w celu zapewnienia zgodności z Ramami i:

- Główny przedmiot działalności Podmiotu OE działającego jako Administrator Danych lub Podmiot Przetwarzający Dane stanowi Przetwarzanie Danych, które, biorąc pod uwagę jego charakter, zakres oraz/lub cel(-e), wymaga regularnego i systematycznego monitorowania Osób Fizycznych (np. retargetowanie drogą e- mailową; działania marketingowe oparte na danych; Profilowanie i scoring na potrzeby oceny ryzyka (np. na potrzeby scoringu kredytowego, ustalenia składek ubezpieczeniowych, zapobiegania oszustwom czy wykrywania przypadków prania pieniędzy); śledzenie lokalizacji; reklama behawioralna; monitorowanie danych dotyczących kondycji i sprawności fizycznej oraz zdrowia za pomocą urządzeń noszonych na ciele; urządzenia skomunikowane (np. inteligentne liczniki, inteligentne samochody czy automatyka domowa) na duża skalę (np. Przetwarzanie Danych Osobowych klientów na potrzeby ustalenia składek ubezpieczeniowych);
- Główny przedmiot działalności Podmiotu OE działającego jako Administrator Danych lub Podmiot Przetwarzający Dane stanowi Przetwarzanie, na dużą skalę, Wrażliwych Danych Osobowych, a także Danych Osobowych dotyczących wyroków skazujących i przestępstw (por. Rozdział B, Dział IV ust. 2 — ust. 2 pkt. 2 oraz ust. 2 pkt. 3); lub
- Wymagają tego stosowne przepisy i regulacje.

Oceniając, czy Inspektor Ochrony Danych musi zostać wyznaczony, jak opisano powyżej, dany Zarząd Podmiotu OE musi udokumentować taką ocenę w celu umożliwienia wykazania, że zostały uwzględnione istotne czynniki, oraz zaktualizować taką ocenę, gdy jest to niezbędne (np. jeżeli Podmiot OE podejmie nowy przedmiot działalności łub będzie świadczyć nowe usługi, które mogą być objęte przypadkami wymienionymi powyżej).

Dany Zarząd Podmiotu OE musi zapewnić, że Inspektor Ochrony Danych:

- Jest powoływany zgodnie z wymogami stosownych przepisów i regulacji obowiązujących w EOG oraz/lub organów ochrony danych działających na terenie EOG;
- Bezpośrednio podlega Zarządowi Podmiotu OE;
- Właściwie i terminowo angażuje się we wszelkie kwestie dotyczące prywatności i ochrony danych, tzn. Inspektor Ochrony Danych musi być uwzględniany jako partner w dyskusji odnośnie spraw dotyczących operacji Przetwarzania Danych i jego opinie należy traktować z należytą powagą. Wszelkie odstępstwa od jego porad muszą zostać udokumentowane;
- Posiada odpowiednie zasoby i nieograniczony dostęp do operacji Przetwarzania Danych oraz utrzymuje poziom posiadanej wiedzy fachowej;
- Nie otrzymuje poleceń dotyczących wykonywania powyższych zadań;
- Jest objęty ochroną przed zwolnieniem z pracy i karą za wykonywane przez siebie zadania;

- Jest związany klauzulą tajemnicy lub poufności odnośnie wykonywanych przez siebie zadań zgodnie ze stosownymi przepisami i regulacjami obowiązującymi w EOG;
- Wykonuje wszelkie inne zadania i obowiązki wyłącznie, gdy nie powodują one Konfliktu interesów (np. Inspektor Ochrony Danych nie może pełnić w Podmiocie OE funkcji, w ramach której ustala cele i sposoby Przetwarzania Danych Osobowych);
- Upubliczni swoje dane kontaktowe i przekaże swoje imię i nazwisko i dane kontaktowe głównemu organowi ochrony danych działającemu na terenie EOG do dnia 25 maja 2018 roku oraz powiadomi główny organ ochrony danych działający na terenie EOG o wszelkich zmianach tych danych zaistniałych w późniejszym terminie; oraz
- Jest osiągalny dla Osób Fizycznych (np. lokalizacja na terenie UE w stosownych przypadkach) we wszelkich kwestiach dotyczących Przetwarzania ich Danych Osobowych i korzystania z ich praw.

2. Specjalista ds. Prywatności Danych/Inspektor Ochrony Danych Podmiotu OE

2.1. Globalne obowiązki

Dany Specjalista ds. Prywatności Danych/Inspektor Ochrony Danych Podmiotu OE:

- Zapewnia odpowiednie wdrożenie niniejszego SOPA na poziomie Podmiotu OE;
- Zapewnia, że procesy przestrzegania prywatności i ochrony danych są odpowiednio wdrażane, utrzymywane i przestrzegane zgodnie z poszczególnymi wymogami wewnętrznymi i zewnętrznymi;
- Udziela porad Pracownikom w zakresie ich praw i obowiązków wynikających z niniejszego SOPA;
- Współpracuje z Dyrektorem Grupy ds. Prywatności lub GC/Działem Prywatności Ochrony Danych Grupy na potrzeby:
  - Rozstrzygnięcia wszelkich konfliktów między postanowieniami niniejszego SOPA a lokalnymi przepisami i regulacjami, aby ustalić odpowiednie działania, a, w przypadku wątpliwości, konsultacji z organami ochrony danych działającymi na terenie EOG;
  - Wyjaśnienia zakresu lub zastosowania jakiejkolwiek części niniejszego SOPA;
  - Reagowania na incydenty Utraty Danych Osobowych rozpatrywania Wniosków Podmiotów Danych o Uzyskanie Dostępu; oraz
  - zgłaszania znaczących braków w zakresie prywatności i ochrony danych w Podmiocie OE;
- Współpracuje z lokalnymi organami ochrony danych, organami regulacyjnymi i organami władzy; oraz
- Współpracuje z Dyrektorem Grupy ds. Prywatności lub innymi Podmiotami OE przy rozpatrywaniu wniosków lub skarg Osób Fizycznych lub w przypadku prowadzonych przez organ ochrony danych działający na terenie EOG dochodzeń lub zapytań składanych przez taki organ.

2.2. Dodatkowe obowiązki dotyczące przetwarzania danych w EOG i przekazywania danych zgodnie z WRK

Specjalista ds. Prywatności Danych/Inspektor Ochrony Danych Podmiotu OE:

- W razie incydentu Utraty Danych Osobowych (w tym wycieku danych zgodnie

z Rozdziałem B, Dział VIII niniejszego SOPA) ocenia i wypełnia, zgodnie z Dyrektywami bezpieczeństwa informacji w Allianz, Standardem odporności operacyjnej w Allianz i wszelkimi innymi politykami i standardami Allianz, które mogą mieć zastosowanie, i, w stosownych przypadkach, określone prawne obowiązki dokonywania zgłoszeń i bezzwłocznie informuje Dyrektora Grupy ds. Prywatności (lub, w stosownych przypadkach, umożliwia powiadomienie Dyrektora Grupy ds. Prywatności poprzez stanowiska w regionie lub globalnych liniach związane z prywatnością) o wszelkich potwierdzonych incydentach Utraty Danych Osobowych;

- Przestrzega wszelkich dodatkowych obowiązków, w tym dotyczących Oceny Wpływu na Prywatność, określonych w dowolnej części Zasad Funkcjonalnych Ram;
- Współpracuje i stosuje się do porad wszelkich organów ochrony danych działających na terenie EOG w zakresie interpretacji Wymogów wobec przekazywania danych zgodnie z WRK;
- Ocenia każdy wyrok lub postanowienie sądu, trybunału lub organu administracyjnego spoza EOG wymagające przekazania lub ujawnienia Danych EOG w celu zapewnienia, że takie przekazanie lub ujawnienie danych jest prowadzone zgodnie ze stosownymi przepisami i regulacjami obowiązującymi w EOG;
- Okresowo weryfikuje Wymogi wobec przekazywania danych zgodnie z WRK w stosunku do stosownych przepisów i regulacji, które mogą powstrzymać go od wypełniania swoich obowiązków wynikających z niniejszego SOPA; a, w dozwolonym zakresie, bezzwłocznie informuje o tym Dyrektora Grupy ds. Prywatności, aby ustalić odpowiednie działania, a, w przypadku wątpliwości, skonsultować się z organami ochrony danych działającymi na terenie EOG i wszelkimi innymi istotnymi interesariuszami; oraz
- Niezależnie rozpatruje skargi Osób Fizycznych dotyczące Przekazywania danych zgodnie z WRK i postępuje zgodnie z procedurą określoną w Załączniku D, Dział II. (Rozpatrywanie wniosków osób fizycznych dotyczących przetwarzania danych w EOG oraz skarg dotyczących przekazywania danych zgodnie z WRK).

Ponadto, Inspektor Ochrony Danych:

- Współpracuje z właściwymi organami ochrony danych działającymi na terenie EOG i działa jako ich punkt kontaktowy w kwestiach dotyczących Przetwarzania Danych w EOG, w tym w zakresie uprzednich konsultacji odnośnie Ocen Wpływu na Prywatność; oraz
- Wykonując swoje obowiązki, w należyty sposób uwzględnia ryzyko związane z Przetwarzaniem Danych, mając na uwadze charakter, zakres, kontekst i cel(-e) Przetwarzania Danych.

3. Kierownik ds. Prywatności Projektu

W przypadku każdego programu lub projektu obejmującego gromadzenie oraz/lub Przetwarzanie Danych Osobowych, sponsor programu lub kierownik projektu musi ustalić konieczność, jeśli taka istnieje, powołania Kierownika ds. Prywatności Projektu, jeżeli Specjalista ds. Prywatności Danych/Inspektor Ochrony Danych Podmiotu OE nie zdecyduje się pełnić tej funkcji. Kierownik ds. Prywatności Projektu:

- Współpracuje ze Specjalistą ds. Prywatności Danych/Inspektorem Ochrony Danych Podmiotu OE;

- Zapewnia właściwe uwzględnienie Ram i stosownych regulacji podczas fazy planowania i wdrażania; oraz
- Udziela wsparcia Specjaliście ds. Prywatności Danych/Inspektorowi Ochro Danych Podmiotu OE przy przeprowadzaniu Ocen Wpływu na Prywatność projektu.

4. Właściciel Informacji

Na potrzeby Ram własność Danych Osobowych jest związana z zawodową i biznesową odpowiedzialnością jednostki organizacyjnej w konkretnej kwestii. Jednostka organizacyjna tworząca lub uruchamiająca tworzenie lub przechowywanie Danych Osobowych jest właścicielem takich Danych Osobowych i jest reprezentowana przez kierownika takiej jednostki organizacyjnej („Właściciel Informacji"). W zakresie, w jakim dotyczy to sfery odpowiedzialności Właściciela Informacji, Właściciel Informacji zapewnia:

- Przestrzeganie wymogów Ram;
- Gromadzenie i Przetwarzanie Danych Osobowych wyłącznie w zakresie, w jakim jest to wymagane dla realizacji określonego, jednoznacznego i uzasadnionego celu biznesowego;
- Jasne przyznanie i udokumentowanie własności Danych Osobowych oraz odpowiednią identyfikację i klasyfikację takich Danych Osobowych; oraz
- Sprecyzowanie i stosowanie odpowiednich i określonych kontroli prywatności i ochrony danych w całym cyklu życia Danych Osobowych (obejmującym ich zgromadzenie lub utworzenie, przechowywanie, Przetwarzane, przekazywanie i utylizację) oraz regularną weryfikację takich kontroli pod kątem ich adekwatności i skuteczności.

III. Grupa Allianz i kierowanie podmiotami OE

1. Społeczność ds. Prywatności i Ochrony Danych w Allianz

Specjaliści ds. Prywatności Danych/Inspektorzy Ochrony Danych Podmiotów OE wchodzą w skład globalnej Społeczności ds. Prywatności i Ochrony Danych w Allianz. Społeczność ds. Prywatności i Ochrony Danych podlega Działowi Prywatności i Ochrony Danych Grupy i jest przez niego koordynowana w celu zapewnienia kompleksowego objęcia Prywatnością i Ochroną Danych całej Grupy Allianz.

2. Grupa Doradcza Allianz ds. Prywatności

Podmioty OE, regiony i globalne linie są reprezentowane w Grupie Doradczej Allianz ds. Prywatności. Cel i skład Grupy Doradczej Allianz ds. Prywatności bardziej szczegółowo opisano w podlegającym zmianom Zakresie zadań i obowiązków Grupy Doradczej Allianz ds. Prywatności.

F. Odniesienia do innych dokumentów

Niniejszy SOPA stanowi część Ram prywatności danych Allianz, które obejmują również podlegające zmianom poniższe dokumenty:

- Zasadę funkcjonalną ocen wpływu na prywatność i dokumentacji przetwarzania danych, Zasadę funkcjonalną rozpatrywania wniosków podmiotów danych o uzyskanie dostępu,

Zasada funkcjonalna zarządzania incydentami dotyczącymi danych osobowych. Ramy może zostać uzupełniona o inne Zasady funkcjonalne.

Ponadto, niniejszy SOPA został uzupełniony o podlegające zmianom poniższe dokumenty:

- Politykę zgodności Grupy Allianz
- Standard bezpieczeństwa informacji w Allianz
- Standard zarządzania dokumentami w Allianz
- Dyrektywy bezpieczeństwa informacji w Allianz
- Standard odporności operacyjnej w Allianz.

Szczegółowe informacje są dostępne przez Allianz Connect w Księdze reguł korporacyjnych.

Załącznik A: Słownik terminów

Term in	Opis
Grupa Allianz	Oznacza Allianz SE i każdy podmiot pozostający, bezpośrednio lub pośrednio, w całości lub w części własnością Allianz SE (z wyłączeniem przedsiębiorstw stowarzyszonych i podmiotów typu joint venture).
Grupa Doradcza Allianz ds. Prywatności	Oznacza organ doradczy i kierowniczy ustanowiony w celu wsparcia zastosowania zrównoważonego poziomu prywatności i ochrony danych w Grupie Allianz w drodze opracowania i wdrożenia działań projektów i inicjatyw związanych z prywatnością i ochroną danych.
Wiążące Reguły Korporacyjne lub WRK	Oznaczają prawnie uznany mechanizm legalizacji i umożliwiania przekazywania Danych Osobowych pochodzących z EOG lub tam przetwarzanych w ramach grupy przedsiębiorstw.
Przekazywanie Danych zgodnie z WRK	Oznacza ujawnienie Danych EOG, w drodze fizycznego przekazania danych lub dostępu na odległość, Podmiotom OE spoza EOG, które są stroną Umowy Międzyzakładowej.
Administrator Danych	Oznacza osobę fizyczną lub prawną, organ władzy publicznej, agencję lub inny organ, który, samodzielnie lub wspólnie z innymi, ustala cele („dlaczego") i sposoby („jak") Przetwarzania Danych Osobowych. Jeżeli dwóch lub więcej Administratorów Danych wspólnie ustala cele í sposoby Przetwarzania Danych, uznaje się ich za współadministratorów, którzy współpracują w przejrzysty sposób w celu zapewnienia przestrzegania niniejszego SOPA.
Podmiot Przetwarzający Dane	Oznacza osobę fizyczną lub prawną Przetwarzającą Dane Osobowe w imieniu Administratora Danych.
EOG	Oznacza kraje należące do Unii Europejskiej oraz Islandię, Liechtenstein i Norwegię.
Dane EOG	Dane EOG odnoszą się do Przetwarzanych Danych Osobowych, których Przetwarzanie podlega obowiązkowi przestrzegania przepisów i regulacji obowiązujących w EOG.
Przetwarzanie Danych w EOG	Przetwarzanie Danych w EOG oznacza Przetwarzanie Danych Osobowych podlegających obowiązkowi przestrzegania przepisów regulacji w zakresie prywatności i ochrony danych obowiązujących u EOG, tzn. w przypadkach gdy: ▪ Dane Osobowe są Przetwarzane w kontekście czynności podejmowanych przez przedsiębiorstwo Administratora Danych lub Podmiotu Przetwarzającego Dane na terenie EOG, nawet jeżeli samo Przetwarzanie Danych nie zachodzi w EOG; lub ▪ Dane Osobowe Osób Fizycznych przebywających na terenie EOG są Przetwarzane w celu złożenia Osobom Fizycznym ofert na towary lub usługi lub w celu monitorowania ich zachowania.
Pracownicy	Oznaczają pracowników, kierowników, dyrektorów i członków zarządu Podmiotu OE.
Ramy	Oznaczają niniejszy Standard ochrony prywatności w Allianz (‚SOPA") i odpowiednie Zasady funkcjonalne.

Dyrektor Grupy ds. Prywatności	Oznacza kierownika Działu Prywatności i Ochrony Danych Grupy w Grupie Allianz powoływanego przez Zarząd Allianz SE
Dział Prywatności i Ochrony Danych Grupy	Oznacza Dział Prywatności i Ochrony Danych Grupy w Allianz SE
Osoba Fizyczna	Oznacza zidentyfikowaną lub możliwą do zidentyfikowania osobę fizyczną, której dotyczą Dane Osobowe. Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można zidentyfikować, bezpośrednio lub pośrednio, szczególnie przez odniesienie do identyfikatora, np. nazwiska, numeru identyfikacyjnego, danych dotyczących lokalizacji, identyfikatora online lub przynajmniej jednego czynnika charakterystycznego dla fizycznej, fizjologicznej, genetycznej, umysłowej, ekonomicznej kulturowej lub społecznej tożsamości takiej osoby fizycznej. W odniesieniu do niniejszego SOPA oznacza ona Pracowników personel powiązany, klientów, partnerów handlowych lub jakiekolwiek inne strony trzecie, których Dane Osobowe są Przetwarzane, jak dalej opisano w Załączniku B.
Właściciel Informacji	Oznacza kierownika jednostki organizacyjnej tworzącej lub uruchamiającej tworzenie lub przechowywanie Danych Osobowych.
Umowa Międzyzakładowa	Oznacza umowę międzyzakładową podpisaną przez podmioty prawne Grupy Allianz w celu nadania mocy prawnej niniejszemu SOPA.
Podmioty OE	Oznaczają skonsolidowane podmioty zarządzające i ich poszczególne podmioty prawne w Grupie Allianz (z wyłączeniem podmiotów stowarzyszonych i podmiotów typu joint venture).
Dane Osobowe	Oznaczają wszelkie informacje dotyczące Osoby Fizycznej.
Utrata Danych Osobowych	Oznacza wszelkie przypadki utraty, wycieku lub naruszenia danych które obejmują lub mogą obejmować Dane Osobowe.
Ocena Wpływu na Prywatność	Oznacza ustrukturyzowaną i powtarzalną analizę wykorzystania Danych Osobowych zapewniającą informacje identyfikujące oceniające i łagodzące ryzyko związane z prywatnością i ochroną danych oraz opisujące odpowiednie i proporcjonalne środki zmniejszania wpływu i prawdopodobieństwa ryzyka związanego z prywatnością i ochroną danych, obejmujące środki organizacyjne i techniczne (np. regulacje, procedury, wytyczne, umowy prawne praktyki zarządcze lub struktury organizacyjne).
Przetwarzanie Danych	Oznacza każdą operację lub ciąg operacji dokonywanych na Danych Osobowych lub na zestawach Danych Osobowych przy pomocy środków zautomatyzowanych lub innych, jak np. zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptacja lub modyfikacja, pobieranie, uzyskiwanie wglądu, wykorzystywanie, ujawnianie poprzez przekazywanie, rozpowszechnianie lub udostępnianie w inny sposób, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
Profilowanie	Oznacza każdą formę automatycznego przetwarzania Danych Osobowych polegającą na wykorzystaniu Danych Osobowych celu dokonania oceny określonych osobistych aspektów dotyczących Osoby Fizycznej, szczególnie analizy lub przewidywania

	aspektów dotyczących wyników pracy, sytuacji finansowej, zdrowia, osobistych preferencji, zainteresowań odpowiedzialności, zachowania, lokalizacji lub ruchów takiej Osoby.
Wnioski Podmiotów Danych o Uzyskanie Dostępu	Oznaczają korzystanie przez Osoby Fizyczne z ich praw dotyczących Przetwarzania ich Danych Osobowych, jak przewidują stosowne przepisy i regulacje (np. prawa do dostępu zgłaszania sprzeciwu).
Wrażliwe Dane Osobowe	Oznaczają Dane Osobowe ujawniające pochodzenie rasowe lub etniczne, opinie polityczne, przekonania religijne lub filozoficzne lub przynależność do związków zawodowych oraz Przetwarzanie danych genetycznych i biometrycznych, na potrzeby niepowtarzalnej identyfikacji Osoby Fizycznej, danych dotyczących zdrowia lub danych dotyczących życia seksualnego lub orientacji seksualnej osoby fizycznej.

Załącznik B: Przekazywanie danych zgodnie z WRK objęte niniejszym SOPA

I. Kategorie osób fizycznych

Wymogi wobec przekazywania danych zgodnie z WRK zawarte w niniejszym SOPA obejmują następujące kategorie Osób Fizycznych:

- Obecnych, dawnych i przyszłych Pracowników, w tym, między innymi, osoby zatrudnione w pełnym i niepełnym wymiarze czasu pracy, pracowników przejściowych i sezonowych; pracowników pobierających pensję, konsultantów, wykonawców i pracowników tymczasowych; praktykantów i stażystów; kandydatów; krewnych pracowników („Dane Kadrowe").
- Obecnych, dawnych i przyszłych klientów indywidualnych i biznesowych oraz przedstawicieli klientów indywidualnych i biznesowych, a także inne strony trzecie (np. osoby zgłaszające roszczenia, beneficjentów, osoby wnoszące skargę, osoby składające zapytania oraz członków i beneficjentów systemu emerytalnego) („Dane Klientów").
- Obecnych, dawnych i przyszłych agentów, brokerów i pośredników; dostawców towarów í usług; powierników systemu emerytalnego; udziałowców; i wszelkich innych partnerów handlowych („Dane Stron Trzecich").

II. Kategorie danych osobowych

Wymogi wobec przekazywania danych zgodnie z WRK zawarte w niniejszym SOPA obejmują następujące kategorie Danych Osobowych:

- **Dane Kadrowe** - w tym, między innymi, podstawowe dane osobowe (np. imię i nazwisko; wiek i data urodzenia); wykształcenie, doświadczenie i przynależność zawodowa (np. historia wykształcenia i szkoleń; znajomość języków obcych; przynależność do związków zawodowych); informacje o podróżach pracowników i o ich kosztach (np. dane dotyczące rezerwacji; wymogi dietetyczne; dane paszportowe i dotyczące wiz); sytuacja rodzinna i socjalna oraz tryb życia (np. stan cywilny; dane kontaktowe do osób w razie sytuacji awaryjnej; religia lub przekonania religijne); podstawowe dane kadrowe (np. nazwa stanowiska pracy i funkcja; lokalizacja biura; dzień rozpoczęcia pracy); informacje dotyczące zdrowia, dobrostanu i nieobecności (np. powody nieobecności; niepełnosprawność, dostęp, informacje dotyczące szczególnych wymagań); informacje dotyczące wydajności pracowników (np. postępowania dyscyplinarne, ocena wydajności); dane finansowe (np. dane konta bankowego; numer ubezpieczenie społecznego; wypłaty premii; informacje fotograficzne, nagrania i informacje dotyczące lokalizacji (np. obrazy z kamer przemysłowych; dane dotyczące monitorowania); kontrole w zakresie identyfikacji i dokładne sprawdzanie (np. wyniki kontroli pod kątem karalności; dowód kwalifikowalności do podjęcia pracy).
- **Dane Klientów** - w tym, między innymi, podstawowe dane osobowe (np. imię i nazwisko, wiek i data urodzenia); przedmiot działalności gospodarczej (np. świadczone usługi); sytuacja rodzinna i socjalna oraz

tryb życia (np. osoby na utrzymaniu, małżonek, partner, informacje dotyczące rodziny; religia lub przekonania religijne; wyroki skazujące i przestępstwa); informacje dotyczące zdrowia, dobrostanu i nieobecności (np. dane dotyczące zdrowa fizycznego i psychicznego lub stanu chorobowego; zażalenia i skargi); dane finansowe (np. dane konta bankowego; numer ubezpieczenie społecznego); informacje fotograficzne, nagrania i informacje dotyczące lokalizacji (np. obrazy z kamer przemysłowych); kontrole w zakresie identyfikacji i dokładne sprawdzanie (np. wyniki kontroli pod kątem karalności; dane dotyczące sprawdzenia zdolności kredytowej).

- Dane Stron Trzecich - w tym, między innymi, podstawowe dane osobowe (np. imię i nazwisko); przedmiot działalności gospodarczej (np. dostarczane towary lub usługi); dane finansowe (np. dane konta bankowego); informacje fotograficzne, nagrania i informacje dotyczące lokalizacji (np. obrazy z kamer przemysłowych); kontrole w zakresie identyfikacji i dokładne sprawdzanie (np. wyniki kontroli pod kątem karalności).

III. Cele przetwarzania danych

Wymogi wobec przekazywania danych zgodnie z WRK zawarte w niniejszym SOPA obejmują każdy rodzaj Przetwarzania Danych i następujące cele:

- **Dane kadrowe**: zarządzanie zasobami ludzkimi, w tym, między innymi, ogólne zarządzanie stosunkiem pracy (np. lista płac), rekrutacja, zarządzanie talentami, kształcenie i rozwój kadry (np. szkolenia), bezpieczeństwo i ochrona, zarządzanie motywacją, zapobieganie zagrożeniom w miejscu pracy (tj. zagrożeniom związanym ze zdrowiem, pracą i otoczeniem), zarządzanie usługami wsparcia informatycznego; relacje w pracy (np. relacje z radą zak1adową); wewnętrzne zarządzanie działaniami wspierającymi (np. prawne; audyt wewnętrzny); zarządzanie ciągłością działalności (ciągłość oraz planowanie kryzysowe i reagowanie na kryzys); przestrzeganie zobowiązań prawnych (np. zgłaszanie naruszeń).
- **Dane klientów**: zarządzanie relacjami z klientami, w tym, między innymi, usługi sprzedażowe i obsługa klienta, fakturowanie, marketing, komunikacja, podatki, zarządzanie informatyczne, rozpatrywanie reklamacji; rozpatrywanie roszczeń ubezpieczeniowych; rozpatrywanie roszczeń z tytułu ubezpieczenia zdrowotnego lub na życie; zarządzanie emeryturami kapitałowymi lub planami emerytalnymi; zarządzanie portfelem aktywów; zarządzanie nieruchomościami; operacje; wewnętrzne zarządzanie działaniami wspierającymi (np. prawne; audyt wewnętrzny); sprawozdawczość; przestrzeganie zobowiązań prawnych (np. w dziedzinie przeciwdziałania praniu pieniędzy); bezpieczeństwo i ochrona.
- **Dane Stron Trzecich**: zarządzanie relacjami z partnerami, w tym, między innymi, zarządzanie umowami z agentami, zarządzanie emeryturami kapitałowymi lub planami emerytalnymi, zarządzanie informatyczne, zarządzanie motywacją; wewnętrzne zarządzanie działaniami wspierającymi (np. prawne; audyt wewnętrzny); administracja i sprawozdawczość wewnętrzna; bezpieczeństwo i ochrona.

Załącznik C: Wymogi minimalne odnośnie umów zawieranych między administratorem danych a podmiotem przetwarzającym dane o przetwarzanie danych w EOG i przekazywanie danych zgodnie z WRK

W przypadku Przetwarzania Danych w EOG i Przekazywania Danych zgodnie z WRK Podmioty OE działające jako Administratorzy Danych muszą włączyć następujące wymogi w razie zawierania umów z Podmiotami Przetwarzającymi Dane (innym Podmiotem OE lub stroną trzecią nienależącą do Grupy Allianz) zgodnie z Rozdziałem B, Dział V ust. 2.

Postanowienia odnoszące się do Przetwarzania Danych w EOG:

- ✓ Przedmiot I okres Przetwarzania Danych;
- ✓ Charakter i cel Przetwarzania Danych; oraz
- ✓ Rodzaj Danych Osobowych i kategorie Osób Fizycznych

Prawa i obowiązki Administratora Danych:

- ✓ Obowiązki Podmiotu OE działającego jako Administrator Danych; oraz
- ✓ Prawa Podmiotu OE działającego jako Administrator Danych

Zobowiązania Podmiotu Przetwarzającego Dane:

- ✓ Przetwarzanie Danych Osobowych wyłącznie na udokumentowane polecenie Administratora Danych, obejmujące przekazywanie danych do krajów spoza EOG;
- ✓ Zawiadamianie o wszelkich przepisach i regulacjach obowiązujących w EOG, które mają zastosowanie do Podmiotu Przetwarzającego Dane i wymagają od niego Przetwarzania Danych Osobowych wychodzącego poza zakres objęty poleceniem Administratora Danych, chyba że takie informacje są zabronione z uwagi na ważny interes publiczny;
- ✓ Zapewnienie udzielenia zezwoleń na przetwarzanie Danych Osobowych wyłącznie osobom związanym zobowiązaniem do zachowania poufności lub odpowiednim ustawowym obowiązkiem zachowania poufności;
- ✓ Podejmowanie wszelkich niezbędnych środków bezpieczeństwa gwarantujących spełnianie przez Przetwarzanie Danych wymogów określonych w Rozdziale B, Dział VII. ust. 2 niniejszego SOPA;
- ✓ Angażowanie Podwykonawców Przetwarzania Danych wyłącznie po uprzednim uzyskaniu pisemnego ogólnego lub szczególnego upoważnienia Administratora Danych;
- ✓ W przypadku udzielenia przez Administratora Danych pisemnego ogólne upoważnienia informowanie Administratora Danych o wszelkich planowany zmianach dotyczących angażowania nowych lub zastępowania Podwykonawców Przetwarzania Danych łącznie z możliwością zgłoszenia sprzeciwu wobec takich zmian;
- ✓ Przenoszenie swoich obowiązków w zakresie prywatności i ochrony danych na Podwykonawców Przetwarzania Danych na mocy umowy lub innego aktu prawnego

bez zwalniania się z odpowiedzialności wobec Administratora Danych, w tym z tytułu naruszenia lub niewypełnienia zobowiązania przez Podwykonawców Przetwarzania Danych;

- ✓ Udzielanie wsparcia Administratorowi Danych za pomocą odpowiednich środków technicznych i organizacyjnych uwzględniających charakter Przetwarzania Danych i w zakresie, w jakim to możliwe, przy wypełnianiu obowiązku Administratora Danych udzielania odpowiedzi na wnioski o korzystanie przez Osoby Fizyczne z ich praw;
- ✓ Udzielanie wsparcia Administratorowi Danych w zapewnianiu przestrzegania jego obowiązków dotyczących ochrony, powiadamiania organów ochrony danych działających na terenie EOG oraz/lub Osób Fizycznych o naruszeniach oraz Ocen Wpływu na Prywatność z uwzględnieniem charakteru Przetwarzania Danych i informacji dostępnych Podmiotowi Przetwarzającemu Dane;
- ✓ Wedle uznania Administratora Danych - usunięcie lub zwrot Administratorowi Danych wszystkich Danych Osobowych pod koniec świadczenia wszelkich usług dotyczących Przetwarzania Danych oraz usunięcie istniejących kopii, chyba że stosowne przepisy i regulacje obowiązujące w EOG wymagają przechowywania Danych Osobowych; oraz
- ✓ Udostępnianie Administratorowi Danych wszelkich informacji niezbędnych do wykazania przez niego przestrzegania obowiązków zgodnie ze stosownymi przepisami i regulacjami obowiązującymi w EOG oraz umożliwienie i wkład w audyty, obejmujące kontrole, przeprowadzane przez Administratora Danych lub innego audytora upoważnionego przez Administratora Danych; oraz bezzwłoczne informowanie Administratora Danych jeżeli, jego zdaniem, polecenie narusza stosowne przepisy i regulacje obowiązujące w EOG.

Załącznik D: Rozpatrywanie wniosków osób fizycznych dotyczących przetwarzania danych w EOG oraz skarg dotyczących przekazywania danych zgodnie z WRK

Procedura określona w niniejszym Załączniku D ma zastosowanie do Danych EOG w odniesieniu do wniosków Osób Fizycznych zgłaszanych na mocy Rozdziału D, Działy 1. do V. oraz skarg Osób Fizycznych dotyczących naruszenia Wymogów wobec przekazywania danych zgodnie z WRK złożonych na mocy Rozdziału C, Dział III.

I. Wnioski osób fizycznych dotyczące przetwarzania danych w EOG

Podmioty mioty OE działające jako Administratorzy Danych muszą umożliwić korzystanie przez Osoby Fizyczne z praw do uzyskania dostępu, sprostowania lub usunięcia danych czy zgłaszania sprzeciwu, ograniczenia lub przenoszalności danych oraz praw dotyczących zautomatyzowanych decyzji indywidualnych (obejmujących Profilowanie).

1. Potwierdzenie tożsamości osoby fizycznej

W przypadkach gdy Podmioty OE działające jako Administratorzy Danych wyrażą uzasadnione wątpliwości dotyczące tożsamości Osoby Fizycznej skradającej wniosek lub gdy wymagają tego stosowne przepisy i regulacje obowiązujące w EOG, Podmioty OE mogą zażądać dostarczenia dodatkowych informacji niezbędnych dla potwierdzenia tożsamości Osoby Fizycznej z wyjątkiem sytuacji, gdy wniosek dotyczy zautomatyzowanych decyzji indywidualnych (obejmujących Profilowanie).

2. Terminy rozpatrywania wniosków

Podmioty OE działające jako Administratorzy Danych:

- Muszą dostarczyć Osobie Fizycznej informacje dotyczące każdego działania podjętego w następstwie złożonego przez nią wniosku bez zbędnej zwłoki, ale nie później niż w ciągu 1 miesiąca od daty otrzymania wniosku;
- Mogą wydłużyć termin na udzielenie odpowiedzi Osobie Fizycznej o kolejne 2 miesiące, uwzględniając złożoność i zakres wniosku i muszą poinformować Osobę Fizyczną o każdym wydłużeniu terminu w ciągu 1 miesiąca od daty otrzymania wniosku z podaniem powodów opóźnienia; oraz
- Muszą poinformować Osobę Fizyczną bez zbędnej zwłoki, ale nie później niż w ciągu 1 miesiąca od daty otrzymania wniosku o podjęciu decyzji o nierozpatrywaniu wniosku Osoby Fizycznej z podaniem powodów takiej decyzji oraz o prawie Osoby Fizycznej do złożenia skargi do organu regulacyjnego ochrony danych działającego na terenie EOG i wykorzystania środków prawnych.

3. Forma odpowiedzi udzielonej osobie fizycznej

Jeżeli Osoba Fizyczna złoży wniosek drogą elektroniczną, Podmiot OE działający jako Administrator Danych musi udzielić informacji drogą elektroniczną i, tam, gdzie to możliwe, w powszechnie stosowanej formie elektronicznej, chyba że Osoba Fizyczna zażąda inaczej.

4. Koszty

Jakikolwiek przekaz informacji czy działanie podjęte przez Podmiot OE działający jako Administrator Danych w następstwie skorzystania przez Osobę Fizyczną ze swoich praw musi nastąpić bezpłatnie poza przypadkami, gdy możliwe jest pobranie uzasadnionej opłaty, tzn. jeżeli:

- Wniosek jest wyraźnie bezpodstawny lub przesadny, w szczególności z powodu jego powtarzalnego charakteru, w którym to przypadku Podmiot OE działający jako

Administrator Danych ponosi ciężar wykazania wyraźnie bezpodstawnego lub przesadnego charakteru wniosku; lub
- Wniosek dotyczy kolejnych kopii Danych Osobowych Osoby Fizycznej.

5. Odmowa podjęcia działania w odpowiedzi na wniosek osoby fizycznej

Podmioty OE działające jako Administratorzy Danych mogą odmówić podjęcia działań w odpowiedzi na wnioski, gdy:

- Są one wyraźnie bezpodstawne lub przesadne, w szczególności z powodu ich powtarzalnego charakteru, a Podmioty OE mogą wykazać wyraźnie bezpodstawny lub przesadny charakter wniosków;
- Przetwarzanie Danych nie wymaga identyfikacji, a Podmioty OE mogą wykazać, że nie są w stanie zidentyfikować Osoby Fizycznej; lub
- Stosowne przepisy i regulacje obowiązujące w EOG wyraźnie ograniczają prawo Osoby Fizycznej.

W przypadku wniosku o usunięcie Danych Osobowych Podmioty OE działające jako Administratorzy Danych mogą również odmówić podjęcia działań w odpowiedzi na wnioski, jeżeli Przetwarzanie Danych jest niezbędne dla:

- Korzystania z prawa swobody wypowiedzi i wolności informacji;
- Przestrzegania przepisów i regulacji obowiązujących w EOG, którym podlega Administrator Danych, a które wymagają Przetwarzania Danych, lub na potrzeby wykonania zadania podejmowanego w interesie publicznym lub wykonywania uprawnień publicznych powierzonych Administratorowi Danych; lub
- Ustalenia, realizacji lub obrony roszczeń prawnych,

6. Powiadamianie odbiorców

Jeżeli wniosek dotyczy praw do sprostowania lub usunięcia Danych Osobowych lub ograniczenia Przetwarzania Danych, Podmioty OE działające jako Administratorzy Danych muszą poinformować o każdym przypadku sprostowania lub usunięcia Danych Osobowych albo ograniczenia Przetwarzania Danych każdego odbiorcę, któremu ujawniono Dane Osobowe, chyba że okaże się to niemożliwe lub wiąże się to z niewspółmiernym wysiłkiem.

Na wniosek Osoby Fizycznej Podmioty OE działające jako Administratorzy Danych muszą poinformować Osobę Fizyczną o takich odbiorcach.

II. Skargi osób fizycznych dotyczące naruszenia Wymogów wobec przekazywania zgodnie z WRK

Podmioty OE działające jako Administratorzy Danych muszą przestrzegać procedury określonej poniżej w przypadku każdej skargi Osoby Fizycznej dotyczącej naruszenia Wymogów wobec przekazywania zgodnie z WRK, na mocy których Dane Osobowe Osoby Fizycznej są przekazywane Podmiotom OE spoza EOG.

Taką skargę Osoba Fizyczna składa, przesyłając wiadomość e-mailową na adres: privacy@allianz.com.

Specjalista ds. Prywatności Danych/Inspektor Ochrony Danych Podmiotu OE kieruje rozpatrywaniem skarg na początku Przetwarzania Danych i musi:

- Przesłać potwierdzenie otrzymania skargi Osoby Fizycznej w ciągu 2 tygodni od jej

otrzymania i podać Osobie Fizycznej procedurę i terminy udzielenia odpowiedzi; Zbadać i zrozumieć okoliczności Przetwarzania Danych podlegającego skardze oraz zebrać informacje istotne dla udzielenia odpowiedzi na skargę;

- Dążyć do rozstrzygnięcia skargi oraz udzielenia Osobie Fizycznej odpowiedzi w każdym przypadku jak najszybciej, ale nie później niż w ciągu 2 miesięcy od daty otrzymania skargi;
- Bezzwłocznie przekazać skargę Dyrektorowi Grupy ds. Prywatności, jeżeli w toku dochodzenia Specjalista ds. Prywatności Danych/Inspektor Ochrony Danych Podmiotu OE spodziewa się, że nie da się zachować 2-miesięcznego terminu na udzielenie odpowiedzi, oraz poinformować o tym Osobę Fizyczną z podaniem oczekiwanego terminu rozpatrzenia skargi przez Dyrektora Grupy ds. Prywatności (przy czym taki okres nie może być dłuższy niż 2 miesiące od daty przekazania skargi Dyrektorowi Grupy ds. Prywatności);
- W przypadku, gdy wyniki dochodzenia wykażą, że skarga jest uzasadniona - współpracować z Zarządem Podmiotu OE i Dyrektorem Grupy ds. Prywatności, odpowiednio, w celu wdrożenia odpowiednich środków dla rozstrzygnięcia skargi oraz poinformować Osobę Fizyczną o wynikach dochodzenia i odpowiednich środkach naprawczych, a także o możliwości przekazania skargi Dyrektorowi Grupy ds. Prywatności w przypadku braku zadowolenia z wyniku rozpatrzenia skargi;
- W przypadku, gdy wyniki dochodzenia wykażą, że skarga jest nieuzasadniona - poinformować Osobę Fizyczną o wynikach oraz o możliwości przekazania skargi Dyrektorowi Grupy ds. Prywatności w razie zamiaru zakwestionowania takich wyników; oraz
- W każdym przypadku - poinformować Osobę Fizyczną o jej prawie do złożenia skargi do właściwego sądu lub organu ochrony danych działającego na terenie EOG, np. gdy nie jest ona zadowolona z uzyskanej odpowiedzi.

Załącznik E: Przegląd wymogów zawartych w SOPA

		Globalne wymogi minimalne	Wymogi wobec przetwarzania danych w EOG	Wymogi wobec przekazywania danych zgodnie z WRK
A.	**Wprowadzenie**			
I.	Uzasadnienie	1	2	3
II.	Uprawnienia I aktualizacje	1	2	3
B.	**Zasady przestrzegania prywatności i ochrony danych**			
I.	Należyta staranność	1	2	3
II.	Jakość danych			
1.	Ograniczenie celu			
1.1.	*Globalne wymogi minimalne*	1	2	3
1.2.	*Wymogi dodatkowe wobec przetwarzania danych w EOG I przekazywania danych zgodnie z WRK*		2	3
2.	Minimalizacja i dokładność danych	1	2	3
3.	Ograniczenie przechowywania	1	2	3
III.	Przejrzystość i otwartość			
1.	Globalne wymogi minimalne	1	2	3
2.	Warunki udzielania zgody na przetwarzanie danych w EOG i przekazywania danych zgodnie z WRK			
2.1.	*Informacje zbierane od osób fizycznych*		2	3
2.2.	*Informacje niezbierane od osób fizycznych*		2	3
IV.	Legalność przetwarzania danych			
1.	Globalne wymogi minimalne	1	2	3
2.	Warunki udzielania zgody na przetwarzanie danych w EOG I przekazywania danych zgodnie z WRK		2	3
3.	Legalność przetwarzania wrażliwych danych osobowych w przypadku przetwarzania danych w EOG i przekazywania danych zgodnie z WRK		2	3
4.	Legalność przetwarzania danych o wyrokach skazujących i przestępstwach w przypadku przetwarzania danych w EOG i przekazywania danych zgodnie z WRK		2	3
V.	Stosunki w podmiotami przetwarzającymi dane			
1.	Globalne wymogi minimalne	1	2	3
2.	Wymogi dodatkowe wobec przetwarzania danych w EOG i przekazywania danych zgodnie z WRK		2	3
VI.	Przekazywanie danych i dalsze przekazywania danych			
1.	Globalne wymogi minimalne	1	2	3
2.	Wymogi dodatkowe wobec przetwarzania danych w EOG I przekazywania danych zgodnie z WRK		2	3
VII.	Bezpieczeństwo i poufność danych			
1.	Globalne wymogi minimalne	1	2	3
2.	Wymogi dodatkowe wobec przetwarzania danych w EOG i przekazywania danych zgodnie z WRK		2	3
VIII.	Utrata danych osobowych			
1.	Globalne wymogi minimalne	1	2	3

2.	Wymogi dodatkowe wobec przetwarzania danych w EOG i przekazywania danych zgodnie z WRK		2	3
2.1.	*Powiadamianie właściwego organu ochrony danych działającego na terenie EOG*		2	3
2.2.	*Powiadamianie osób fizycznych*		2	3
2.3.	*Powiadamianie Administratora Danych*		2	3
IX.	Ochrona prywatności w fazie projektowania i domyślna ochrona prywatności			
1.	Ochrona prywatności w fazie projektowania			
1.1.	*Globalne wymogi minimalne*	1	2	3
1.2.	*Wymogi dodatkowe wobec przetwarzania danych w EOG i przekazywania danych zgodnie z WRK*		2	3
2.	Domyślna ochrona prywatności w przypadku przetwarzania danych w EOG i przekazywania danych zgodnie z WRK		2	3
X.	Współpraca z właściwymi organami ochrony danych działającymi na terenie EOG w zakresie przetwarzania danych w EOG i przekazywania danych zgodnie z WRK		2	3

C.	**Czynności i procesy dotyczące przestrzegania prywatności i ochrony danych**			
I.	Dokumentacja operacji przetwarzania danych	1	2	3
II.	Szkolenia			
1.	Globalne wymogi minimalne	1	2	3
2.	Wymogi dodatkowe wobec przekazywania danych zgodnie z WRK			3
III.	Wewnętrzny mechanizm rozpatrywania skarg			
1.	Globalne wymogi minimalne	1	2	3
2.	Wymogi dodatkowe wobec przekazywania danych zgodnie z WRK			3
IV.	Ocena wpływu na prywatność	1	2	
V.	Monitorowanie i zapewnienie zgodności			
1.	Globalne wymogi minimalne		2	3
2.	Wymogi dodatkowe wobec przekazywania danych zgodnie z WRK			3

D.	**Obowiązki wobec osób fizycznych**			
I.	Udzielanie odpowiedzi na wnioski osób fizycznych o uzyskanie dostępu, sprostowanie lub usunięcie danych			
1.	Globalne wymogi minimalne	1	2	3
2.	Wymogi dodatkowe wobec przetwarzania w EOG i przekazywanie danych zgodnie z WRK		2	3
2.1.	*Prawo dostępu do danych*		2	3
2.2.	*Prawo do sprostowania danych*		2	3
2.3.	*Prawo do usunięcia danych*		2	3
II.	Udzielanie odpowiedzi na wnioski osób fizycznych dotyczących sprzeciwu wobec przetwarzania danych w EOG i przekazywania danych zgodnie z WRK		2	3
III.	Udzielanie odpowiedzi na wnioski osób fizycznych o ograniczenie przetwarzania danych w EOG i przekazywania danych zgodnie z WRK		2	3
IV.	Udzielanie odpowiedzi na wnioski osób fizycznych o umożliwienie przenoszalności danych odnośnie przetwarzania danych w EOG i przekazywania danych zgodnie z WRK		2	3
V.	Udzielanie odpowiedzi na wnioski osób fizycznych dotyczących sprzeciwu wobec zautomatyzowanych decyzji w sprawie przetwarzania danych w EOG i przekazywania danych zgodnie z WRK		2	3

E.	**Podział ról I obowiązków**			
I.	Poziom Grupy Allianz			
1.	Zarząd Allianz SE	1	2	3
2.	Dział Prywatności o Ochrony Danych Grupy	1	2	3
3.	Dyrektor Grupy ds. Prywatności	1	2	3
II.	Poziom podmiotów OE Allianz			
1.	Zarząd Podmiotu OE			
1.1.	*Globalne Obowiązki*	1	2	3
1.2.	*Dodatkowe obowiązki dotyczące przetwarzania danych w EOG i przekazywania danych zgodnie z WRK*		2	3
2.	Specjalista ds. Prywatności Danych Podmiotu OE			
2.1.	*Globalne Obowiązki*	1	2	3
2.2.	*Dodatkowe obowiązki dotyczące przetwarzania danych w EOG i przekazywania danych zgodnie z WRK*		2	3
3.	Kierownik ds. Prywatności Projektu	1	2	3
4.	Właściciel Informacji	1	2	3
III.	Grupa Allianz I kierowanie podmiotami OE	1	2	3
1.	Społeczność ds. Prywatności I Ochrony Danych w Allianz	1	2	3
2.	Grupa Doradcza Allianz ds. Prywatności	1	2	3

F.	**Odniesienia do innych dokumentów**	1	2	3

Załącznik A	**Słownik terminów**	1	2	3
Załącznik B	**Przekazywanie danych zgodnie z WRK objęte niniejszym SOPA**			3
Załącznik C	**Wymogi minimalne odnośnie umów zawieranych między administratorek danych a podmiotem przetwarzającym dane o przetwarzanie danych w EOG i przekazywanie danych zgodnie z WRK**		2	3
Załącznik D	**Rozpatrywanie wniosków osób fizycznych dotyczących przetwarzania danych w EOG oraz skarg dotyczących przekazywania danych zgodnie z WRK**			
I.	Wnioski osób fizycznych dotyczących przetwarzania danych w EOG		2	3
II.	Skargi osób fizycznych dotyczących naruszenia Wymogów wobec przekazywania danych zgodnie z WRK			3

Informacje o dokumencie

Nazwa dokumentu:	Standard ochrony prywatności w Allianz (SOPA)
Autorzy:	Philipp Räther, Kully Thandi
Osoba kontaktowa:	Dział Prywatności o Ochrony Danych
Obszar Stosowanie:	Allianz Group

Amendments and Updates

Version	Date	Reason for and Extent of Changes	Author(s)
2.0	10-04-2018	Przyjęcie WRK przez Grupę Allianz. Niniejszy dokument zastępuje Standardy Ochrony Prywatności danych w Allianz z dnia 1 Października 2013.	Philipp Räther, Kully Thandi