KODEKS POSTĘPOWANIA

w zakresie podnoszenia poziomu ochrony danych osobowych w działalności członków Izby Zarządzających Funduszami i Aktywami (IZFiA)

Warszawa, dnia 21 maja 2018 roku

Spis treści

I Definicje

§1

1. **Administrator** – oznacza podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania Danych Osobowych, w szczególności Fundusz Inwestycyjny, Towarzystwo Funduszy Inwestycyjnych lub Agenta Transferowego w zakresie w jakim nie jest Podmiotem Przetwarzającym.
2. **Agent Transferowy (AT)** – podmiot świadczący usługi polegające na prowadzeniu rejestru uczestników Funduszy Inwestycyjnych reprezentowanych przez Towarzystwa Funduszy Inwestycyjnych.
3. **Dane Osobowe, Dane** – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
4. **Dłużnik** – podmiot zobowiązany do zaspokojenia wierzytelności będącej przedmiotem lokat Funduszu Sekurytyzacyjnego.
5. **Dystrybutor** – podmiot za pośrednictwem którego Fundusz Inwestycyjny zbywa i odkupuje jednostki uczestnictwa, tytuły uczestnictwa lub certyfikaty inwestycyjne.
6. **Fundusz Inwestycyjny** – podmiot zdefiniowany w art. 3 ust. 1 Ustawy o funduszach inwestycyjnych.
7. **Fundusz Sekurytyzacyjny** – Fundusz Inwestycyjny zdefiniowany w art. 183 ust. 1 Ustawy o funduszach inwestycyjnych.
8. **Izba Zarządzających Funduszami i Aktywami, IZFiA** – izba gospodarcza zrzeszająca Towarzystwa Funduszy Inwestycyjnych oraz domy maklerskie prowadzące działalność wyłącznie w zakresie doradztwa inwestycyjnego albo zarządzania portfelami w skład, których wchodzi jeden lub większa liczba instrumentów finansowych, w której z głosem doradczym uczestniczą również Agenci Transferowi.
9. **Naruszenie Ochrony Danych Osobowych** – oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do Danych Osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
10. **Odbiorca –** osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest Stroną Trzecią. Odbiorcami w szczególności nie są osoby, które z upoważnienia Administratora lub Podmiotu Przetwarzającego mogą przetwarzać Dane Osobowe.
11. **Podmiot Danych** – oznacza potencjalnego, aktualnego lub byłego:
    a) uczestnika Funduszu Inwestycyjnego,
    b) pełnomocnika, osobę uposażoną, spadkobiercę uczestnika Funduszu Inwestycyjnego, beneficjenta rzeczywistego lub inne osoby powiązane,
    c) Dłużnika lub inną osobę, której Dane Administrator przetwarza w związku z prowadzeniem działalności oraz w związku z realizacją obowiązków i uprawnień wskazanych we właściwych przepisach prawa, mających zastosowanie do Administratora oraz w aktach wewnętrznych takich jak statuty.
12. **Podmiot Przetwarzający –** osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza Dane Osobowe w imieniu Administratora. Podmiotem Przetwarzającym może być w szczególności Agent Transferowy.
13. **Podmioty Stosujące Kodeks** – podmioty, o których mowa w §2 ust. 2 i 7 poniżej.
14. **Rozporządzenie, RODO** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
15. **Strona Trzecia** – osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, Administrator, Podmiot Przetwarzający czy osoby, które – z upoważnienia Administratora lub Podmiotu Przetwarzającego – mogą przetwarzać Dane Osobowe.
16. **Towarzystwo Funduszy Inwestycyjnych (TFI)** – podmiot, o którym mowa w art. 4 oraz Dziale III Ustawy o funduszach inwestycyjnych.
17. **Ustawa o funduszach inwestycyjnych** – ustawa z dnia 27 maja 2014 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi (t.j. Dz. U. z 2018 r., poz. 56 z późn. zm.)
18. **Zgoda** – oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej Danych Osobowych.

II Postanowienia ogólne

§2

1. Stosowanie Kodeksu postępowania stanowi potwierdzenie wywiązywania się z obowiązków nałożonych przez Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych) na Administratorów oraz Podmioty Przetwarzające, które działają na rynku Funduszy Inwestycyjnych i są członkami lub podmiotami wspierającymi IZFiA.
2. Kodeks postępowania ma zastosowanie do członków lub podmiotów wspierających IZFiA, działających na terytorium Rzeczpospolitej Polskiej, które zobowiązały się do przestrzegania zasad w nim określonych poprzez złożenie IZFiA pisemnego oświadczenia. Kodeks postępowania został sporządzony z uwzględnieniem specyfiki funkcjonowania polskiego rynku Funduszy Inwestycyjnych.
3. Kodeks postępowania stanowi doprecyzowanie zasad przetwarzania i ochrony Danych Osobowych na podstawie art. 40 RODO, w zakresie podnoszenia poziomu ochrony Danych Osobowych i rekomendowanych działań przez IZFiA, które obejmują w szczególności:
   a) rzetelne i przejrzyste przetwarzanie;
   b) prawnie uzasadnione interesy realizowane przez Podmioty Stosujące Kodeks w określonych kontekstach;
   c) zbieranie Danych Osobowych w konkretnych, wyraźnych i prawnie uzasadnionych celach;
   d) pseudonimizację Danych Osobowych;
   e) wykonywanie przez Podmioty Danych przysługujących im praw;
   f) środki i procedury regulujące obowiązki Podmiotów Stosujących Kodeks oraz ochronę Danych Osobowych w fazie projektowania i domyślną ochronę Danych Osobowych;
   g) środki i procedury zapewniające bezpieczeństwo przetwarzania;
   h) zgłaszanie organowi nadzorczemu naruszeń ochrony Danych Osobowych oraz zawiadamianie o takich naruszeniach Podmiotów Danych.
4. Mając na uwadze znaczenie Kodeksu postępowania dla ochrony Danych Osobowych w działalności polskiego rynku Funduszy Inwestycyjnych, członkowie i podmioty wspierające IZFiA deklarują współpracę na rzecz:
   a) podnoszenia poziomu ochrony Danych Osobowych w działalności polskiego rynku Funduszy Inwestycyjnych,
   b) upowszechniania i jednolitego wdrażania zasad prawnej ochrony Danych Osobowych,
   c) zwiększania zaufania Podmiotów Danych.
5. Mając na uwadze specyfikę działalności poszczególnych członków IZFiA oraz różnice w zakresie uwarunkowań, skali działalności i profili ryzyka, szczegółowe działania w zakresie ochrony Danych Osobowych mogą być realizowane odmiennie przy zachowaniu podstawowych wymagań opisanych w niniejszym Kodeksie postępowania oraz zgodnych z wymaganiami RODO.
6. Kodeks postępowania ma zastosowanie do przetwarzania Danych Osobowych Podmiotów Danych, a nie dotyczy przetwarzania Danych Osobowych pracowników, współpracowników oraz kandydatów do pracy w Podmiotach Stosujących Kodeks.
7. Inne podmioty, niż wskazane w ust. 2, przystępując do stosowania Kodeksu postępowania zobowiązują się do przestrzegania zasad w nim określonych poprzez złożenie pisemnego oświadczenia do IZFiA.
8. Towarzystwa Funduszy Inwestycyjnych i Fundusze Inwestycyjne nie świadczą usług społeczeństwa informacyjnego bezpośrednio dzieciom, z uwagi na obowiązek reprezentowania ich przez przedstawicieli ustawowych.

III Zasady przetwarzania Danych Osobowych

§3

Podmioty Stosujące Kodeks przetwarzają Dane Osobowe Podmiotów Danych:

1. **W sposób zgodny z prawem, rzetelny** - w szczególności w oparciu o przepisy powszechnie obowiązującego prawa regulujące funkcjonowanie Podmiotów Stosujących Kodeks, wskazane w §7 poniżej.
2. **W konkretnych, wyraźnych i prawnie uzasadnionych celach** - w szczególności w oparciu o **zasadę celowości**, tj.:

1) w celu wykonania umowy o uczestnictwo w Funduszach Inwestycyjnych lub podjęcia działań na żądanie Podmiotu Danych, przed zawarciem tej umowy,
2) w celu wypełnienia obowiązku prawnego ciążącego na Administratorze,
3) w celu wynikającym z prawnie uzasadnionych interesów realizowanych przez Administratora lub przez Stronę Trzecią, za które uznaje się w szczególności:
   a) marketing bezpośredni usług i produktów oferowanych przez Administratora, w tym Towarzystwo Funduszy Inwestycyjnych i zarządzane przez nie Fundusze Inwestycyjne,
   b) prowadzenie marketingu bezpośredniego usług i produktów innych podmiotów (marketing cudzych produktów i usług),
   c) dochodzenie i obrona przed roszczeniami,
   d) prowadzenie statystyk,
   e) ochronę przed próbami oszustwa,
   f) bezpieczeństwo świadczonych usług, w tym bezpieczeństwo teleinformatyczne oraz wyjaśnianie okoliczności niedozwolonego korzystania z usług,
   g) przesyłanie Danych w ramach grupy kapitałowej,
   h) przesyłanie Danych w ramach grupy przedsiębiorstw do wewnętrznych celów administracyjnych,
   i) stosowanie systemów kontroli wewnętrznej.

Zapewnienie, by Dane były przetwarzane zgodnie z zasadą celowości realizowane jest poprzez spełnienie wymagań obowiązku informacyjnego, wskazanie okresu przetwarzania lub sposobu jego wyliczania, odpowiedni nadzór, przypisanie odpowiedzialności, a także realizację procesów i procedur wewnętrznych.

3. **Adekwatnie do celów, w których są przetwarzane –** w szczególności w oparciu o **zasadę minimalizacji Danych**, która polega na przetwarzaniu Danych adekwatnych, stosownych oraz ograniczonych do celów przetwarzania. Zapewnienie, by Dane były przetwarzane zgodnie z zasadą adekwatności realizowane jest już na etapie pozyskiwania Danych, a także w procesach tworzenia i modyfikowania nowych usług, procesów oraz systemów informatycznych.
4. **Z zachowaniem prawidłowości Danych Osobowych** – w szczególności poprzez podejmowanie rozsądnych działań, aby zbierane Dane Osobowe były poprawne i w razie potrzeby uaktualniane, a w przypadkach w których są nieprawidłowe do celów przetwarzania, zostały niezwłocznie usunięte lub sprostowane. Zapewnienie przestrzegania **zasady merytorycznej poprawności** Danych jest realizowane zgodnie z zasadami zarządzania Danymi, w tym przede wszystkim zarządzania architekturą oraz jakością Danych.
5. **W formie umożliwiającej identyfikację Podmiotu Danych przez okres nie dłuższy niż jest to niezbędne –** w szczególności w oparciu o **zasadę ograniczenia przechowywania Danych** przez okres nie dłuższy niż to jest niezbędne do celów przetwarzania, a po tym okresie usuwania, anonimizowania lub trwałego niszczenia danych. Zapewnienie przestrzegania tej zasady jest realizowane w ramach wewnętrznych mechanizmów kontrolnych, procesów i procedur Administratora.
6. **W sposób zapewniający odpowiednie bezpieczeństwo Danych Osobowych –** w szczególności w oparciu o **zasadę integralności i poufności**, która polega na zabezpieczeniu Danych za pomocą odpowiednich środków technicznych lub organizacyjnych zapewniających ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem, przypadkową utratą Danych, zniszczeniem lub ich uszkodzeniem, niezależnie od formy przetwarzania Danych i z uwzględnieniem analizy ryzyka.
7. **W sposób zapewniający rozliczalność –** w szczególności w oparciu o **zasadę rozliczalności**, która umożliwia wykazanie, że zostały wdrożone i są przestrzegane zasady dotyczące przetwarzania Danych Osobowych ze szczególnym uwzględnieniem domyślnej ochrony Danych oraz ochrony Danych w fazie projektowania, a także dokumentowanie przestrzegania zasad ochrony Danych Osobowych.
8. **W sposób przejrzysty –** w szczególności w oparciu o **zasadę przejrzystości**, która polega na przekazywaniu Podmiotom Danych informacji w sposób łatwo dostępny, zrozumiały oraz sformułowany jasnym i prostym językiem. Zasada ta jest realizowana zarówno w zakresie informowania o tożsamości Administratora, celach przetwarzania, ale także innych obowiązkach dotyczących przetwarzania Danych Osobowych wskazanych w RODO.

IV Podstawy przetwarzania Danych Osobowych

§4

Podstawy przetwarzania

Podmioty Stosujące Kodeks przetwarzają Dane Osobowe, jeżeli spełniony jest co najmniej jeden z poniższych warunków:

1. Podmiot Danych wyraził Zgodę na przetwarzanie swoich Danych Osobowych w jednym lub większej liczbie określonych celów.
2. Przetwarzanie jest niezbędne do wykonania umowy, której stroną jest Podmiot Danych, lub do podjęcia działań na żądanie Podmiotu Danych przed zawarciem umowy.

3. Przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze.
4. Przetwarzanie jest niezbędne do ochrony żywotnych interesów Podmiotu Danych lub innej osoby fizycznej.
5. Przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej.
6. Przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub przez Stronę Trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności Podmiotu Danych wymagające ochrony Danych Osobowych, w szczególności gdy Podmiot Danych jest dzieckiem.

§5

Przetwarzanie na podstawie Zgody

1. W przypadku, gdy podstawą przetwarzania Danych Osobowych ma być Zgoda Podmiotu Danych, Zgoda powinna zostać wyrażona poprzez złożenie ustnego, pisemnego lub elektronicznego oświadczenia woli lub poprzez wyraźne działanie potwierdzające, którego treścią jest przyzwolenie na przetwarzanie Danych Osobowych Podmiotu Danych, pod warunkiem wcześniejszego potwierdzenia tożsamości Podmiotu Danych. Nie wyłącza to uprawnienia Podmiotu Danych do wyrażenia Zgody w innej akceptowalnej i możliwej do udokumentowania przez Administratora formie.
2. Zgoda może być odebrana w szczególności z wykorzystaniem papierowego formularza podpisanego przez Podmiot Danych, w formie elektronicznego formularza na stronie internetowej lub w systemie informatycznym z polami wyboru do kliknięcia poprzez zaznaczenie okienka wyboru, poprzez wybór ustawień technicznych systemu informatycznego lub strony internetowej, z wykorzystaniem poczty elektronicznej lub telefonu (sms, nagranie rozmowy telefonicznej).
3. Poprzez wyraźne działanie rozumie się zamiar, intencję lub zachowanie, z którego Zgoda jednoznacznie wynika. W szczególności może to być wybór przez Podmiot Danych określonych ustawień technicznych w systemie informatycznym, przekazanie ustne, pisemne lub elektroniczne Danych Osobowych przez Podmiot Danych w celu uzyskania odpowiedzi na zapytanie, przekazanie wizytówki np. w celu wzięcia udziału w konkursie.
4. Przetwarzanie Danych Osobowych w związku ze zautomatyzowanym podejmowaniem decyzji w indywidualnych sprawach, w tym profilowaniem, o którym owa w art. 22 ust. 1 i 4 RODO, przekazywanie Danych Osobowych do państwa trzeciego na podstawie Zgody lub przetwarzanie szczególnych kategorii Danych Osobowych wymaga wyraźnej Zgody, o ile Administrator nie posiada innej podstawy prawnej przetwarzania Danych Osobowych. W takim wypadku Zgoda musi zostać udzielona w formie oświadczenia, a nie poprzez wyraźne działanie.
5. Zapytanie o Zgodę powinno być sformułowane w zrozumiałej, łatwo dostępnej formie, jasnym i prostym językiem, a także dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach.
6. Jeżeli Dane Osobowe mają być przetwarzane w różnych celach (niepowiązanych ze sobą) potrzebne są odrębne Zgody wyrażone przez Podmiot Danych na poszczególne cele.
7. Klauzula Zgody na przetwarzanie Danych Osobowych powinna zawierać co najmniej nazwę i adres Administratora oraz cel (cele), w jakich będzie on przetwarzać Dane Osobowe. Klauzula Zgody może zawierać dodatkowe elementy. Przykładowy wzór klauzuli zawiera Załącznik nr 1 do Kodeksu.
8. Podmiot Danych ma prawo wycofać Zgodę w każdym momencie, przy czym wycofanie Zgody nie wpływa na zgodność z prawem przetwarzania Danych Osobowych, którego dokonano na podstawie Zgody przed jej wycofaniem. Wycofanie Zgody powinno być możliwe w równie prosty sposób, jak jej wyrażenie w zależności od rozwiązań udostępnionych przez Administratora.
9. Weryfikacja tożsamości może obejmować cyfrową identyfikację Podmiotu Danych, np. poprzez mechanizm uwierzytelniania, taki jak te same dane uwierzytelniające, których Podmiot Danych używa w celu zalogowania się do usług internetowych.
10. W związku z obowiązkiem zachowania zasady rozliczalności przez Podmioty Stosujące Kodeks za przestrzeganie ww. zasady w odniesieniu do przetwarzania Danych Osobowych na podstawie Zgody Podmiotu Danych należy uznać, w szczególności: archiwizowanie pisemnych i elektronicznych oświadczeń woli Podmiotu Danych, rejestrowanie rozmów telefonicznych lub posiadanie skryptów rozmów telefonicznych, dokonywanie kopii zapasowych (back-up'ów lub zrzutów z ekranu), odznaczenie odpowiednich symboli (tick'ów) w bazach danych, posiadanie stosownych polityk i procedur wewnętrznych oraz notatek z przebiegu spotkań.

§6

Przetwarzanie niezbędne do wykonania umowy

1. Przetwarzanie Danych Osobowych Podmiotu Danych jest dopuszczalne jeżeli jest to niezbędne do wykonania umowy gdy Podmiot Danych jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie Podmiotu Danych.
2. Przetwarzanie Danych Osobowych niezbędne do podjęcia działań przed zawarciem umowy na żądanie Podmiotu Danych jest dopuszczalne jeżeli:
   1) przetwarzanie jest niezbędne do podjęcia działań przed zawarciem umowy,
   2) zawarcie umowy następuje na żądanie Podmiotu Danych.

§7

Przetwarzanie niezbędne do wypełnienia obowiązku prawnego

1. Przetwarzanie Danych Osobowych Podmiotu Danych jest dopuszczalne jeżeli:
   1) istnieje przepis prawa, który nakłada na Administratora obowiązek prawny,
   2) przetwarzanie Danych jest niezbędne dla realizacji tego obowiązku prawnego.
2. Przepisy legalizujące przetwarzanie Danych Osobowych przez Podmioty Stosujące Kodeks obejmują w szczególności:
   1) Ustawę z dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi,
   2) Ustawę z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu,
   3) Ustawę z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych,
   4) Ustawę z dnia 9 marca 2017 r. o wymianie informacji podatkowych z innymi państwami,
   5) Ustawę z dnia 9 października 2015 r. o wykonywaniu Umowy między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki w sprawie poprawy wypełniania międzynarodowych obowiązków podatkowych oraz wdrożenia ustawodawstwa FATCA,
   6) Ustawę z dnia 5 sierpnia 2015 r. o rozpatrywaniu reklamacji przez podmioty rynku finansowego i o Rzeczniku Finansowym,
   7) Kodeks Cywilny,
   8) Ustawę z dnia 20 kwietnia 2004 r. o pracowniczych programach emerytalnych,
   9) Ustawę z dnia 20 kwietnia 2004 r. o indywidualnych kontach emerytalnych oraz indywidualnych kontach zabezpieczenia emerytalnego,
   10) Ustawę z dnia 4 lutego 1994 r. o prawach autorskich i prawach pokrewnych,
   11) Ustawę z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną.
3. W przypadku gdy Podmiot Stosujący Kodeks przetwarza Dane Osobowe w zakresie niezbędnym do przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, badania poziomu wiedzy Podmiotu Danych o inwestowaniu w instrumenty finansowe oraz doświadczenie inwestycyjne zgodnie z odrębnymi przepisami, a także zapobiegania przestępstwom, oszustwom lub wykrywaniu oszustw przez właściwe organy, przetwarzanie to nie stanowi zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach, w tym profilowania, o którym mowa w art. 22 ust. 1 i 4 RODO.

§8

Przetwarzanie do celów wynikających z prawnie uzasadnionych interesów

1. Przetwarzanie Danych bez zgody Podmiotu Danych jest dopuszczalne, jeżeli:
   1) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub Stronę Trzecią,
   2) nie zachodzą sytuacje, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności Podmiotu Danych, wymagające ochrony Danych Osobowych, w szczególności gdy Podmiot Danych jest dzieckiem.
2. Przykłady prawnie uzasadnionych interesów przetwarzania Danych Osobowych zostały wskazane w §3 ust. 2 pkt 3) Kodeksu.

V Prawa Podmiotu Danych

§9

Realizacja podstawowych praw Podmiotu Danych

1. Administrator realizuje prawa Podmiotu Danych w szczególności w zakresie:

a) Prawa do informacji (realizacja obowiązku informacyjnego);
b) Prawa dostępu do Danych;
c) Prawa do sprostowania Danych;
d) Prawa do usunięcia Danych („prawo do bycia zapomnianym”);
e) Prawa do ograniczenia przetwarzania;
f) Prawa do przenoszenia Danych;
g) Prawa do sprzeciwu.

2. Powyższe prawa realizowane są przez Administratora w języku polskim, chyba że w komunikacji z Podmiotem Danych standardowo stosowany jest inny język, w sposób przejrzysty, zrozumiały i rzetelny, a także jeżeli to możliwe, z zachowaniem zwięzłej formy i z wykorzystaniem jasnego oraz prostego języka. Dodatkowo przekaz może być ułatwiany poprzez wykorzystanie znaków graficznych, które w widoczny i czytelny sposób przedstawiają sens zamierzonego przetwarzania.
3. Podmiot Danych może wystąpić z żądaniem realizacji praw, o których mowa w ust. 1 korzystając z przyjętych i stosowanych w bieżącej działalności danego Administratora metod kontaktu, takich jak: kanał elektroniczny, Internet (np. STI), telefon (np. IVR), dokumentacja papierowa lub przekaz ustny (bezpośredni).
4. Informacje mogą zostać udzielone przez Administratora, z zastosowaniem obowiązujących standardów bezpieczeństwa:
   a) pisemnie;
   b) ustnie;
   c) w sposób elektroniczny;
   d) w innej formie – akceptowalnej i umożliwiającej udokumentowanie realizacji żądania, w tym z zastosowaniem reguł odnoszących się do postępowań reklamacyjnych, jeżeli nie będą one sprzeczne z Kodeksem.
5. W celu realizacji zgłoszonego żądania lub uprawnienia Podmiotu Danych przez Administratora niezbędne jest:
   a) wcześniejsze zidentyfikowanie osoby składającej wniosek (potwierdzenie tożsamości lub uwierzytelnienie poprzez podanie danych uwierzytelniających), z zachowaniem przyjętych zasad oraz procedur bezpieczeństwa. W razie uzasadnionych wątpliwości co do tożsamości osoby składającej wniosek, Administrator może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, ale nie ma takiego obowiązku,
   b) wskazanie zakresu Danych i czynności, których wniosek dotyczy.
9. Terminy odpowiedzi na żądania lub realizacji praw Podmiotu Danych przez Administratora:
   a) udzielenie informacji o działaniach podjętych w związku z żądaniem realizowane jest bez zbędnej zwłoki, nie później niż w terminie 1 miesiąca od dnia otrzymania żądania.
   b) w uzasadnionych przypadkach, w tym ze względu na skomplikowany charakter żądania lub liczbę żądań, możliwe jest wydłużenie terminu realizacji wniosku o kolejne 2 miesiące, jeżeli nie później niż w terminie 1 miesiąca od dnia otrzymania żądania, udzielana jest informacja o przedłużeniu terminu rozpatrzenia żądania z podaniem przyczyn.
10. Realizacja praw Podmiotu Danych, oraz podejmowanie działań na jego żądanie, są wolne od opłat, z zastrzeżeniem ust. 11.
11. W przypadku ewidentnie nieuzasadnionych lub nadmiernych żądań Podmiotu Danych, w szczególności ze względu na swój ustawiczny charakter, Administrator może pobrać rozsądną opłatę w wysokości uwzględniającej koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań, albo odmówić podjęcia działań w związku z żądaniem.
12. Administrator jest uprawniony do pobrania opłaty, o której mowa w ust. 11 w sytuacji, gdy żądanie:
   a) zostało otrzymane przed upływem 6 miesięcy od dnia zgłoszenia przez Podmiot Danych, żądania tego samego rodzaju, przy czym ograniczenie to nie dotyczy prawa do sprostowania Danych, prawa do usunięcia, prawa do ograniczenia przetwarzania Danych, ani prawa do sprzeciwu;
   b) dotyczy informacji dzielonych na kilka lub kilkanaście żądań;
   c) dotyczy wniosku o szczególny nośnik lub format odpowiedzi, jeżeli nie odpowiada on standardowemu formatowi przyjętemu przez Administratora;
   d) dotyczy wniosku o udzielenie odpowiedzi w języku innym niż język polski, chyba że w komunikacji z Podmiotem Danych standardowo stosowany jest inny język;
   e) dotyczy wniosku, którego realizacja wymaga zaangażowania zasobów ludzkich lub środków niezbędnych do prawidłowego wykonania wniosku w stopniu zakłócającym normalną działalność Administratora, np. wniosku o szczegółowe informacje;
   f) ma zostać zrealizowane w szczególnym trybie jak np. odpowiedź przesłana kurierem.
13. W przypadku, gdy Administrator będzie uprawniony do naliczenia opłaty za realizację wniosku Podmiotu Danych, zgodnie z ust. 11, poinformuje wcześniej Podmiot Danych o wysokości opłaty oraz numerze konta bankowego i rozpocznie realizację wniosku po otrzymaniu takiej opłaty.
14. Administrator jest uprawniony do odmowy podjęcia działań w związku z żądaniem Podmiotu Danych w sytuacji, gdy:

a) żądanie ma zostać zrealizowane w formacie lub na nośniku, który nie jest obsługiwany przez Administratora lub nie spełnia podstawowych standardów bezpieczeństwa;
b) wniosek jest niejasny i nieprecyzyjny, a Podmiot Danych składający wniosek, pomimo prośby o uzupełnienie brakujących informacji, nadal jej nie zrealizował;
c) nie udało się zidentyfikować osoby składającej wniosek - tożsamość nie została ustalona i mimo podjętych prób, nie jest możliwe jej potwierdzenie bez zaangażowania nadmiernych środków, czasu lub działań;
d) Podmiot Danych nie uiścił opłaty, o której mowa w ust. 11 - 13;
e) realizacja żądania mogłaby spowodować ujawnienie tajemnicy zawodowej, Danych Osobowych innej osoby niż wnioskodawca lub naruszenie tajemnicy przedsiębiorstwa Administratora, innej tajemnicy prawnie chronionej lub prawa własności intelektualnej czy też zasad konkurencji.

15. W przypadku, o którym mowa w ust. 14 Administrator informuje o powodach niepodjęcia działań oraz możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.
16. Administrator zapewnia rozliczalność m.in. w zakresie realizacji lub braku realizacji obowiązków względem Podmiotów Danych, w tym obowiązków informacyjnych, w szczególności poprzez zbieranie dokumentów przekazywanych osobom, rejestrację rozmów telefonicznych, rejestrację zdarzeń w systemach informatycznych, kopie bezpieczeństwa, zrzuty z ekranu systemu informatycznego, kopie listów lub wiadomości wysyłanych drogą elektroniczną do Podmiotu Danych, analizy oraz procedury wewnętrzne, skrypty rozmów z Podmiotami Danych.

§10

Realizacja obowiązku informacyjnego

1. Obowiązek informacyjny realizowany jest przez Administratora w przypadku pozyskiwania Danych Osobowych oraz zmiany celów przetwarzania Danych Osobowych w stosunku do celów, dla których Dane Osobowe zostały zebrane.
2. W przypadku pozyskiwania Danych Osobowych zakres informacji przekazywanych Podmiotowi Danych przez Administratora, obejmuje co najmniej:
   a) nazwę, adres, dane kontaktowe oraz, gdy ma to zastosowanie – tożsamość i dane kontaktowe swojego przedstawiciela;
   b) gdy ma to zastosowanie - dane kontaktowe inspektora ochrony danych;
   c) cele przetwarzania Danych;
   d) podstawę prawną przetwarzania Danych;
   e) prawnie uzasadnione interesy realizowane przez Administratora, jeżeli przetwarzanie Danych odbywa się na podstawie art. 6 ust. 1 lit. f) RODO;
   f) informację o Odbiorcach lub kategoriach Odbiorców (jeśli istnieją), którym Dane zostały lub zostaną ujawnione (w szczególności Obiorcy w państwach trzecich lub organizacjach międzynarodowych);
   g) jeżeli ma to zastosowanie, informację o zamiarze przekazania Danych Osobowych do państwa trzeciego na zasadach wskazanych w art. 13 ust. 1 lit. f RODO;
   h) okres, przez który Dane Osobowe będą przechowywane, a gdy nie jest to możliwe – kryteriach ustalania tego okresu;
   i) informację o prawie osoby do żądania od Administratora: dostępu do Danych Osobowych dotyczących Podmiotu Danych, sprostowania Danych, usunięcia Danych, ograniczenia przetwarzania Danych lub o prawie do wniesienia sprzeciwu wobec przetwarzania Danych, a także o prawie do przenoszenia Danych;
   j) informację o prawie do cofnięcia Zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie Zgody przed jej cofnięciem, jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO;
   k) informację o prawie wniesienia skargi do organu nadzorczego;
   l) informację, czy podanie Danych Osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy Podmiot Danych, jest zobowiązany do ich podania i jakie są ewentualne konsekwencje niepodania Danych;
   m) gdy ma to zastosowanie – informację o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 Rozporządzenia, oraz przynajmniej w tych przypadkach istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla Podmiotu Danych.
3. W przypadku pozyskiwania Danych Osobowych nie bezpośrednio od Podmiotu Danych zakres informacji przekazywanych Podmiotowi Danych przez Administratora, obejmuje informacje wskazane w ust. 2 lit. a)-k) i m) oraz dodatkowo:
   a) kategorie odnośnych Danych Osobowych;

b) źródło pochodzenia Danych Osobowych, a gdy ma to zastosowanie - czy pochodzą one ze źródeł publicznie dostępnych.

4. W przypadku zmiany celów przetwarzania Danych Osobowych, zakres informacji przekazywanych Podmiotowi Danych przez Administratora, obejmuje co najmniej:
   a) cele przetwarzania Danych;
   b) okres, przez który Dane Osobowe będą przechowywane, a gdy nie jest to możliwe – kryteriach ustalania tego okresu;
   c) informacje o prawie Podmiotu Danych do żądania od Administratora: dostępu do Danych Osobowych dotyczących Podmiotu Danych, sprostowania Danych, usunięcia Danych, ograniczenia przetwarzania Danych lub o prawie do wniesienia sprzeciwu wobec przetwarzania Danych, a także o prawie do przenoszenia Danych;
   d) informację o prawie do cofnięcia Zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie Zgody przed jej cofnięciem, jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO;
   e) informację o prawie wniesienia skargi do organu nadzorczego;
   f) informację, czy podanie Danych Osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy Podmiot Danych, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania Danych;
   g) gdy ma to zastosowanie – informację o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz przynajmniej w tych przypadkach istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla Podmiotu Danych.
5. W przypadku zmiany celów przetwarzania Danych Osobowych pozyskanych nie bezpośrednio od Podmiotu Danych, zakres informacji przekazywanych Podmiotowi Danych przez Administratora, obejmuje informacje wskazane w ust. 4 lit. a)-e) i g) oraz dodatkowo:
   a) prawnie uzasadnione interesy realizowane przez Administratora, jeżeli przetwarzanie Danych odbywa się na podstawie art. 6 ust. 1 lit. f) RODO;
   b) źródło pochodzenia Danych Osobowych, a gdy ma to zastosowanie - czy pochodzą one ze źródeł publicznie dostępnych.
6. W przypadku zbierania Danych Osobowych bezpośrednio od Podmiotu Danych, informacja jest przekazywana podczas pozyskiwania Danych.
7. W przypadku zbierania Danych Osobowych nie od Podmiotu Danych informacja jest przekazywana:
   a) w rozsądnym terminie, nie później jednak niż w terminie miesiąca od pozyskania Danych;
   b) najpóźniej przy pierwszej komunikacji z Podmiotem Danych, jeżeli Dane Osobowe mają być stosowane do komunikacji z tą osobą;
   c) najpóźniej przy pierwszym ujawnieniu Danych, jeżeli Administrator planuje ujawnić Dane Osobowe innemu Odbiorcy.
6. Klauzule informacyjne mogą być przekazywane z zastosowaniem obowiązujących standardów bezpieczeństwa:
   a) pisemnie;
   b) ustnie;
   c) w sposób elektroniczny;
   d) w innej formie – akceptowalnej i umożliwiającej udokumentowanie realizacji żądania, w tym z zastosowaniem reguł odnoszących się do postępowań reklamacyjnych, jeżeli nie będą one sprzeczne z Kodeksem.
7. Przykładowy wzór klauzuli informacyjnej stanowi Załącznik nr 2 do Kodeksu postępowania.
8. Agenci Transferowi nie spełniają samodzielnie i we własnym zakresie obowiązku informacyjnego w odniesieniu do klientów Funduszy Inwestycyjnych, Towarzystw Funduszy Inwestycyjnych, ponieważ klauzule informacyjne umieszczane są przez Fundusze Inwestycyjne oraz Towarzystwa Funduszy Inwestycyjnych w dokumentach przeznaczonych dla klientów lub w systemie informatycznym po potwierdzeniu tożsamości Podmiotu Danych lub poprzez przesłanie informacji drogą elektroniczną, z zastosowaniem standardów bezpieczeństwa.
9. Obowiązek informacyjny realizowany jest wyłącznie w stosunku do uczestników Funduszy Inwestycyjnych. Obowiązek informacyjny w stosunku do Podmiotów Danych nie jest realizowany przez Administratora, jeżeli:
   a) Podmiot Danych dysponuje już tymi informacjami (np. zbieranie dodatkowych Danych Osobowych w tym samym celu);
   b) udzielenie informacji osobie, której Dane zostały zebrane nie bezpośrednio od niej jest niemożliwe (np. brak adresu) lub wymagałoby niewspółmiernego dużego wysiłku albo wymagałoby pozyskiwania informacji dodatkowych z innych źródeł zewnętrznych. Do takich sytuacji zaliczyć należy m.in. przetwarzanie Danych pełnomocników, przedstawicieli ustawowych, osób uposażonych, beneficjentów rzeczywistych, spadkobierców uczestnika Funduszu Inwestycyjnego lub innych osób powiązanych z uczestnikiem, Danych członków zarządu i reprezentantów zawartych w wyciągach z Krajowego Rejestru Sądowego;
   c) pozyskanie lub ujawnienie Danych osoby, której Dane są zebrane nie bezpośrednio od niej, uregulowane jest w przepisach prawa przewidujących ochronę prawnie uzasadnionych interesów Podmiotu Danych;

d) Dane Osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej, tajemnicy przedsiębiorstwa oraz innych tajemnic ustawowo chronionych.

10. Postanowień ust. 1 – 7 powyżej nie stosuje się wobec Podmiotów Danych, których Dane zostały uzyskane przed dniem 25 maja 2018 roku. Jednakże, jeżeli Administrator uzna za zasadne spełnienie obowiązku informacyjnego względem uczestników Funduszy Inwestycyjnych, którzy zawarli umowę o uczestnictwo przed dniem 25 maja 2018 roku, oraz osób, którym udzielenie informacji okaże się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku obowiązek ten może zostać zrealizowany poprzez umieszczenie informacji na stronie internetowej Towarzystwa Funduszy Inwestycyjnych, w prospekcie informacyjnym bądź emisyjnym lub warunkach emisji.

§11

Prawo dostępu do danych

1. Podmiot Danych jest uprawniony do uzyskania od Administratora potwierdzenia, czy przetwarza on jego Dane Osobowe, a jeżeli ma to miejsce, Podmiot Danych jest uprawniony do uzyskania dostępu do Danych w następującym zakresie:
   a) celów przetwarzania (np. wykonywanie umowy o uczestnictwo w Funduszach Inwestycyjnych, wypełnienie obowiązków prawnych ciążących na Administratorze, realizacja celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora wskazanych w §3 ust. 2 pkt 3 Kodeksu);
   b) kategorii odnośnych Danych Osobowych;
   c) Odbiorcy lub kategorii Odbiorców, którym Dane Osobowe zostały lub mogą zostać ujawnione, w szczególności Odbiorców w państwach trzecich lub organizacjach międzynarodowych (np. Agent Transferowy prowadzący rejestr uczestników Funduszu Inwestycyjnego, depozytariusz, Dystrybutorzy jednostek uczestnictwa, podmioty świadczące usługi doradcze, audytowe, księgowe, informatyczne, archiwizacji i niszczenia dokumentów, marketingowe, jak również biegli rewidenci w związku z audytem);
   d) w miarę możliwości, planowanego okresu przetwarzania Danych Osobowych, a gdy nie jest to możliwe, kryteriów ustalania tego okresu, przy założeniu, iż zapewnione zostanie ograniczenie okresu przechowywania Danych do niezbędnego minimum;
   e) informacji o prawie do żądania sprostowania, usunięcia lub ograniczenia przetwarzania Danych Osobowych dotyczącego Podmiotu Danych, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
   f) informacji o prawie wniesienia skargi do organu nadzorczego;
   g) jeżeli Dane Osobowe nie zostały zebrane od Podmiotu Danych – wszelkich dostępne informacje o ich źródle;
   h) gdy ma to zastosowanie - informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotnych informacji o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla Podmiotu Danych.
2. Jeżeli Dane Osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, Podmiot Danych ma prawo zostać poinformowany o odpowiednich zabezpieczeniach, o których mowa w art. 46 RODO, związanych z przekazaniem, w tym w szczególności o fakcie zatwierdzenia przez organ nadzorczy Kodeksu postępowania.
3. Administrator może udostępnić Podmiotom Danych kanał, w którym Klient będzie mógł samodzielnie pobrać Dane w przypadku żądania Podmiotu Danych dostępu do Danych.
4. Administrator dostarcza Podmiotowi Danych kopię Danych Osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się Podmiot Danych, może zostać pobrana opłata w rozsądnej wysokości wynikająca z kosztów administracyjnych, o których mowa w §9 ust. 11, na zasadach określonych §6 ust. 12-14.
5. Jeżeli Podmiot Danych zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacja zostaje udzielona powszechnie stosowaną drogą elektroniczną o ile możliwe jest uwierzytelnienie lub potwierdzenie tożsamości osoby. W uzasadnionych przypadkach lub jeżeli udostepnienie kopii Danych nie będzie możliwe przez kanał, o którym mowa w ust. 3, przekazanie kopii Danych drogą elektroniczną może być uwarunkowane dodatkowymi wymaganiami uwierzytelnienia lub potwierdzenia tożsamości osoby.

§12

Prawo do sprostowania Danych

1. Podmiot Danych ma prawo żądania od Administratora niezwłocznego sprostowania dotyczących go Danych Osobowych, które są nieprawidłowe.
2. Podmiot Danych ma prawo żądania uzupełnienia niekompletnych Danych Osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia. Przy ocenie zasadności żądania Administrator uwzględnia cel przetwarzania.

3. Administrator, bądź w jego imieniu Podmiot Przetwarzający, informują Podmiot Danych o dokonaniu sprostowania. Potwierdzeniem realizacji prawa do sprostowania Danych może być przyjęcie do realizacji kompletnej i prawidłowej dyspozycji aktualizacji Danych.
4. Informacja o sprostowaniu przekazywana jest Odbiorcom wyłącznie w przypadku gdy nie będzie to wymagało niewspółmiernego wysiłku bądź w sposób oczywisty będzie niemożliwe.
5. Na żądanie Podmiotu Danych Administrator przekazuje informację o Odbiorcach, którym przekazał sprostowane Dane.

§13

Prawo do usunięcia Danych („Prawo do bycia zapomnianym")

1. Każdy Podmiot Danych ma prawo do niezwłocznego usunięcia jego Danych Osobowych przetwarzanych przez Administratora w przypadku:
   1) gdy Dane Osobowe nie są już niezbędne do celów, do których zostały zebrane lub są w inny sposób przetwarzane,
   2) gdy Podmiot Danych cofnął Zgodę, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO i nie ma innej podstawy prawnej przetwarzania,
   3) gdy Podmiot Danych wnosi sprzeciw z przyczyn związanych z jego szczególną sytuacją na mocy art. 21 ust. 1 RODO wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania,
   4) gdy Podmiot Danych wnosi sprzeciw na mocy art. 21 ust. 2 RODO wobec przetwarzania na potrzeby marketingu bezpośredniego, w tym profilowania, w zakresie w jakim przetwarzanie związane jest z profilowaniem,
   5) Dane Osobowe były przetwarzane niezgodnie z prawem,
   6) Dane Osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii Europejskiej lub prawie państwa członkowskiego, któremu podlega Administrator.
2. Administrator nie ma obowiązku usunięcia Danych Osobowych w zakresie w jakim przetwarzanie tych Danych jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń, przetwarzanie jest niezbędne do wywiązania się z prawnego obowiązku, w tym bezpiecznego świadczenia usług i wyjaśniania okoliczności niedozwolonego korzystania z usług.
3. W związku z tym, że Administrator oraz Podmiot Przetwarzający nie upubliczniają Danych Osobowych Podmiotów Danych, nie stosuje się do nich art. 17 ust. 2 RODO.

§14

Prawo do ograniczenia przetwarzania Danych Osobowych

1. Podmiotowi Danych przysługuje prawo do żądania ograniczenia przetwarzania Danych Osobowych od Administratora w następujących przypadkach:
   1) Podmiot Danych kwestionuje prawidłowość Danych Osobowych – na okres pozwalający Administratorowi sprawdzić prawidłowość tych Danych. W szczególności dotyczy to sytuacji, w której Podmiot Danych żąda sprostowania Danych jednocześnie żądając ograniczenia ich przetwarzania;
   2) przetwarzanie jest niezgodne z prawem, a Podmiot Danych sprzeciwia się usunięciu Danych Osobowych, żądając w zamian ograniczenia ich wykorzystywania;
   3) Administrator nie potrzebuje już Danych Osobowych do celów przetwarzania, ale są one potrzebne Podmiotowi Danych do ustalenia, dochodzenia lub obrony roszczeń;
   4) Podmiot Danych wniósł sprzeciw wobec przetwarzania za wyjątkiem sprzeciwu wobec przetwarzania Danych Osobowych na potrzeby marketingu bezpośredniego, w tym związanego z nim profilowania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie Administratora są nadrzędne wobec podstaw sprzeciwu Podmiotu Danych.
2. W przypadku, o którym mowa w ust. 1 pkt 1 Administrator dokonuje niezwłocznej weryfikacji prawidłowości Danych Podmiotu Danych.

3. Z zastrzeżeniem ust. 4, w celu ograniczenia przetwarzania Danych Osobowych Podmiotu Danych, Administrator dokonuje oznaczenia Danych, w sposób, który jest możliwy w systemie, w którym Dane są przetwarzane. Ponadto, w celu ograniczenia przetwarzania Administrator może:
   1) uniemożliwić użytkownikom systemu, w których Dane są przetwarzane, dostęp do wybranych Danych, powyższe oznacza sytuację, w której Podmiot Danych po zalogowaniu się do systemu transakcyjnego nie będzie widział swoich Danych, których przetwarzanie zostało ograniczone w wyniku jego żądania;
   2) ograniczyć środkami technicznymi (np. poprzez czasowe zablokowanie odpowiednich okien) przetwarzania w zautomatyzowanych zbiorach Danych w taki sposób, by Dane Osobowe nie podlegały dalszemu przetwarzaniu ani nie mogły być zmieniane, z zastrzeżeniem że ograniczenie przetwarzania Danych Osobowych musi być wyraźnie zaznaczone w systemie, w którym Dane te są przetwarzane.
4. Administrator może przechowywać Dane Osobowe, co do których zostało zgłoszone żądanie ograniczenia przetwarzania.
5. Jeżeli przetwarzanie Danych Osobowych zostało ograniczone, takie Dane Osobowe Administrator może przetwarzać w inny sposób niż przechowywanie, w następujących przypadkach:
   1) Podmiot Danych wyrazi na to Zgodę, lub
   2) w celu ustalenia, dochodzenia lub obrony roszczeń, lub
   3) w celu ochrony praw innej osoby fizycznej lub prawnej, lub jednostki organizacyjnej niebędącej osobą prawną, której ustawa przyznaje zdolność prawną, lub
   4) z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.
6. Ograniczenie przetwarzania Danych nie powoduje zaprzestania przez Administratora przetwarzania, które jest niezbędne do wykonania przez Administratora obowiązków wynikających z przepisów prawa lub zaleceń lub rekomendacji organów nadzorujących Administratora, w szczególności raportowania na podstawie Ustawy z dnia 9 października 2015 r. o wykonywaniu Umowy między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki w sprawie poprawy wypełniania międzynarodowych obowiązków podatkowych oraz wdrożenia ustawodawstwa FATCA oraz Ustawy z dnia 9 marca 2017 r. o wymianie informacji podatkowych z innymi państwami.
7. W przypadku uchylenia ograniczenia przetwarzania Administrator informuje o tym Podmiot Danych, który żądał ograniczenia przetwarzania jego Danych Osobowych.
8. Złożenie zlecenia po uprzednim zażądaniu ograniczenia przetwarzania Danych Osobowych oznacza Zgodę na dalsze przetwarzanie w rozumieniu art. 18 ust. 2 RODO.

§15

Obowiązek powiadomienia o sprostowaniu lub usunięciu Danych Osobowych lub o ograniczeniu przetwarzania

1. Administrator informuje o sprostowaniu lub usunięciu Danych Osobowych lub ograniczeniu przetwarzania, których Administrator dokonał zgodnie postanowieniami Kodeksu i RODO każdego Odbiorcę, któremu Administrator ujawnił Dane Osobowe Podmiotu Danych.
2. Obowiązek, o którym mowa w ust. 1 nie znajduje zastosowania w sytuacji, gdy po przeprowadzeniu analizy jego wypełnienie okaże się niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku, w szczególności gdy:
   1) Dane zostały ujawnione Odbiorcom w przeszłości i Administrator pomimo podjętych prób nie ma możliwości nawiązania kontaktu z Odbiorcą,
   2) Odbiorca zakończył działalność, w tym jeżeli spółka będąca Odbiorcą została zlikwidowana,
   3) z kontekstu lub okoliczności przetwarzania wynika, że Dane Osobowe nie będą już przetwarzane,
   4) wysiłek włożony w przekazanie informacji przez Administratora jest nieproporcjonalny w stosunku do niedogodności spowodowanych brakiem tych informacji u Podmiotu Danych.
3. Administrator na żądanie Podmiotu Danych informuje go o Odbiorcach, którym ujawnił Dane Osobowe.

§16

Prawo do przenoszenia Danych

1. Podmiot Danych ma prawo do:
   1) otrzymania w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego Danych Osobowych, które dotyczą Podmiotu Danych i które dostarczył Administratorowi;

2) przenoszenia Danych Osobowych, tj. przesłania innemu Administratorowi Danych Osobowych, które dotyczą Podmiotu Danych i które dostarczył Administratorowi, o ile jest to technicznie możliwe i na zasadach określonych w niniejszym Kodeksie.

2. Przez ustrukturyzowany, powszechnie używany format nadający się do odczytu maszynowego rozumiany jest taki format Danych, który umożliwia aplikacjom komputerowym łatwą identyfikację, rozpoznawanie i pozyskanie Danych. Administrator stosuje powszechnie używany format wskazany w Załączniku nr 3 do niniejszego Kodeksu.
3. Podmiot Danych może skorzystać z prawa do otrzymania lub przenoszenia Danych Osobowych, o którym mowa w ust. 1, jeżeli łącznie spełnione są dwa warunki:
   1) przetwarzanie Danych Osobowych odbywa się na podstawie Zgody Podmiotu Danych lub na podstawie umowy, której stroną jest Podmiot Danych;
   2) przetwarzanie Danych Osobowych odbywa się w sposób zautomatyzowany, co oznacza, że Dane Osobowe, które przetwarzane są w sposób tradycyjny, w tzw. zbiorach papierowych (w tym np. skany dokumentów) nie podlegają przenoszeniu.
4. Katalog Danych Osobowych podlegających przenoszeniu został wskazany w Załączniku nr 3 do niniejszego Kodeksu. Przeniesieniu podlegają Dane aktualne, tj. ostatnie Dane uzyskane lub poprawione przez Podmiot Danych.
5. Prawo do otrzymania lub przenoszenia Danych, o którym mowa w ust. 1 nie może niekorzystnie wpływać na prawa i wolności innych Podmiotów Danych.
6. Administrator może wstrzymać realizację żądania do przenoszenia Danych do czasu uzgodnienia końcowego zakresu żądania oraz złożenia przez Podmiot Danych odpowiednich oświadczeń (zgód) niezbędnych do umożliwienia Administratorowi przekazania Danych innemu Administratorowi.
7. Administrator przed realizacją praw, o których mowa w ust. 1 musi mieć możliwość jednoznacznego potwierdzenia tożsamości Podmiotu Danych żądającego przeniesienia Danych Osobowych. Jednocześnie Administrator jest odpowiedzialny za podjęcie wszelkich środków bezpieczeństwa potrzebnych do zapewnienia, aby Dane Osobowe zostały bezpiecznie przeniesione (np. z zastosowaniem zahasłowanego pliku z przekazaniem hasła odrębnym środkiem komunikacji).
8. Administrator odmawia podjęcia działań zmierzających do wydania lub przeniesienia Danych, jeżeli pomimo podjęcia stosownych działań nie jest w stanie potwierdzić tożsamości wnioskującego, informując o tym Podmiot Danych występujący z żądaniem. W szczególności dotyczy to braku uzyskania dodatkowych informacji umożliwiających identyfikację, o których przedstawienie Administrator wystąpił do Podmiotu Danych.
9. Administrator może odmówić również żądania do przeniesienia Danych, o ile będzie ono miało ewidentnie nieuzasadniony bądź nadmierny charakter:
   1) Podmiot Danych domaga się przeniesienia w formacie innym niż wskazany w Załączniku nr 3 do niniejszego Kodeksu;
   2) ilość i częstotliwość wniosków składanych przez Podmiot Danych wskazuje na inny cel działania osoby uprawnionej niż potrzeba realizacji przysługujących jej praw.
10. Przeniesienie Danych nie wpływa na inne prawa Podmiotu Danych wynikające z ochrony Danych Osobowych, w tym nie powoduje usunięcia Danych u dotychczasowego Administratora, ani zmiany okresu przechowywania Danych.
11. Przenoszenie Danych nie nakłada na Administratora obowiązku zatrzymywania Danych Osobowych dłużej niż określony przez Administratora okres przechowywania wynikający z przepisów.
12. Działania mające na celu realizację żądania przeniesienia Danych Osobowych nie mogą nakładać na Podmioty Stosujące Kodeks dodatkowych obciążeń finansowych, związanych np. z obowiązkiem wprowadzania kompatybilnych technicznie systemów przetwarzania, koniecznością wdrożenia nowych rozwiązań technicznych lub zakupu nowego oprogramowania.

§17

Przenoszenie Danych poprzez przekazanie Podmiotowi Danych

1. W celu realizacji prawa do otrzymywania Danych przez Podmiot Danych Administrator zapewni możliwość zapisania pliku na urządzenie prywatne Podmiotu Danych, co nie wyłącza innego sposobu przekazania Danych, w tym poprzez udostępnienie w elektronicznych kanałach dostępu, zapisanie na płycie CD / DVD lub innym fizycznym nośniku.
2. Administrator może przyjąć rozwiązania mające na celu udzielenie niezbędnych informacji Podmiotowi Danych, aby ten mógł podjąć minimalne działania na rzecz ochrony informacji, które otrzymał, np. Administrator może w ramach dobrych praktyk przekazać krótki opis zawartości przekazywanego pliku z Danymi, podstawowe zasady

bezpiecznego przetwarzania, zalecić odpowiednie środki ochrony, w tym odpowiednie format(y) i środki szyfrowania.

§18

Przenoszenie Danych poprzez przesłanie innemu Administratorowi

1. W przypadku wniosku o przesłanie Danych do innego Administratora, bezpośrednie przesłanie Danych przez Administratora „przekazującego" może mieć miejsce, gdy możliwa jest komunikacja pomiędzy dwoma systemami w sposób zapewniający bezpieczeństwo przesyłanych Danych oraz gdy system Administratora „odbierającego" ma techniczną możliwość odebrania Danych.
2. Przenoszenie Danych pomiędzy Administratorami będącymi Podmiotami Stosującymi Kodeks wiąże się z realizacją umowy o uczestnictwo i nie będzie miało praktycznego zastosowania do momentu jej zawarcia przez Podmiot Danych z Administratorem „odbierającym" Dane. Przesłanie Danych do innego Administratora nie oznacza zawarcia umowy uczestnictwa ani nawiązania jakiegokolwiek stosunku umownego z nowym Administratorem „odbierającym".
3. Na wniosek Podmiotu Danych, Administrator w miarę możliwości przekaże Dane Osobowe wskazane we wniosku innemu Administratorowi. W przypadku wniosku o przesłanie Danych do Administratora, który nie jest Podmiotem Stosującym Kodeks, o ile nie będzie możliwe ustalenie bezpiecznego i bezpośredniego środka przekazania Danych do tego Administratora, należy korzystać z możliwości bezpośredniego przekazywania Danych Osobowych Podmiotowi Danych.
4. Dodatkowo, w celu realizacji wniosku, o którym mowa w ust. 3, Podmiot Danych powinien złożyć oświadczenie o wyrażeniu zgody na przeniesienie Danych do Administratora „odbierającego" i zwolnienie Administratora „przekazującego" z obowiązku zachowania tajemnicy zawodowej w tym zakresie. W przypadku braku takiego oświadczenia, Administrator przekaże Dane bezpośrednio Podmiotowi Danych lub wstrzyma się z realizacją żądania do czasu otrzymania odpowiedniego oświadczenia.
5. Administrator „przekazujący" Dane Osobowe odpowiadający na wniosek Podmiotu Danych o przeniesienie Danych nie ma obowiązku sprawdzenia i weryfikacji jakości Danych przed ich przekazaniem, nie jest zobowiązany do poinformowania osób trzecich, których Dane mogą być zawarte w przenoszonych Danych o wykonaniu takiego żądania i jego treści, a także nie ponosi odpowiedzialności za ich dalsze przetwarzanie przez Podmiot Danych i Administratora „odbierającego".
6. Administrator „odbierający" Dane może odmówić przyjęcia części lub wszystkich Danych i niezwłocznie usunąć, zanonimizować lub zniszczyć przekazane mu Dane w przypadku, gdy przetwarzanie Danych, ocena konkretnego stanu faktycznego lub zestawu Danych może w szczególności powodować naruszenie art. 5 i innych RODO lub innych przepisów powszechnie obowiązującego prawa (np. Dane są nadmierne lub ich zakres nie jest dostosowany do celu przetwarzania).

§19

Prawo do sprzeciwu

1. Podmiot Danych ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania jego Danych Osobowych, jeśli są one przetwarzane przez Administratora w celach:
   1) wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub przez Stronę Trzecią, np. w celu statystycznym, profilowania,
   2) marketingu bezpośredniego, w tym profilowania.
2. Wnosząc sprzeciw wobec przetwarzania, Podmiot Danych powinien określić wobec jakiego konkretnego celu przetwarzania wnosi sprzeciw. W przypadku sprzeciwu wobec przetwarzania, o którym mowa w ust. 1 pkt 1, Podmiot Danych powinien dodatkowo wykazać swoją szczególną sytuację i interes uzasadniający wniesienie sprzeciwu. Administratorowi wolno przetwarzać Dane, co do których Podmiot Danych zgłosił sprzeciw jeżeli wykaże on istnienie ważnych, prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności Podmiotu Danych lub podstaw do ustalenia, dochodzenia lub obrony roszczeń. Do sytuacji, w których Administrator będzie mógł przetwarzać Dane pomimo wniesienia sprzeciwu zaliczyć można w szczególności prawnie uzasadnione interesy realizowane przez Administratora wskazane w § 3 ust. 2 pkt 3 lit. c)-f).
3. W wyniku zgłoszenia sprzeciwu wobec przetwarzania:

1) o którym mowa w ust. 1 pkt 1 - Administrator dokonuje analizy, o której mowa w ust. 4 lub opiera się na wcześniej przeprowadzonej analizie dotyczącej podobnego przypadku, a następnie podejmuje decyzję co do zasadności sprzeciwu,
2) o którym mowa w ust. 1 pkt 2 – Administrator zaprzestaje przetwarzania Danych Osobowych do celów marketingu bezpośredniego, jak również na bazie uprzednio udzielonej Zgody na przesyłanie informacji handlowych wybranymi kanałami komunikacji.

4. Analiza, o której mowa w ust. 3 pkt 1, polega na weryfikacji przez Administratora czy po stronie Podmiotu Danych zachodzi szczególna sytuacja uzasadniająca wniesienie sprzeciwu oraz czy potrzeba ochrony prywatności Podmiotu Danych, tj. interesów, praw i wolności Podmiotu Danych, powinna w konkretnym przypadku przeważyć nad potrzebą przetwarzania tych Danych przez Administratora.
5. Przez czas, który jest niezbędny do dokonania analizy, o której mowa w ust. 4, Administrator na żądanie Podmiotu Danych (o ile takie żądanie zostało złożone), stosuje ograniczenie przetwarzania, o którym mowa w art. 18 ust 1 RODO, na zasadach określonych w § 14 Kodeksu.
6. Jeśli Administrator uzna sprzeciw wobec przetwarzania, o którym mowa w ust. 1 pkt 1 za zasadny – Administrator zaprzestaje przetwarzania Danych Osobowych w celach określonych w sprzeciwie.
7. Jeśli Administrator uzna sprzeciw wobec przetwarzania, o którym mowa w ust. 1 pkt 1 za niezasadny – Administrator zawiadomi o tym Podmiot Danych wnoszący sprzeciw i w przystępny sposób wyjaśni mu przyczyny, dla których uznał sprzeciw za niezasadny.

VI Obowiązki Administratora

§20

Analiza ryzyka

1. Sposób realizacji obowiązków RODO nałożonych na Administratora jest uzależniony od ogólnej analizy ryzyka przetwarzania Danych uwzględniającej charakter, zakres, kontekst i cele przetwarzania Danych oraz ryzyko naruszenia praw i wolności Podmiotów Danych, oraz ryzyka naruszenia interesów Administratora. Celem analizy ryzyka jest przegląd i ocena adekwatności zastosowanych przez Administratora środków technicznych i organizacyjnych
2. Sposób przeprowadzenia ogólnej analizy ryzyka powinien zostać odpowiednio opisany, a jej wyniki udokumentowane.
3. W procesie wykonywania ogólnej analizy ryzyka wyróżniamy następujące etapy: identyfikacja, pomiar i ocena prawdopodobieństwa wystąpienia określonego zdarzenia będącego naruszeniem oraz skutków wystąpienia tego ryzyka, metody zarządzania zidentyfikowanym ryzykiem.
4. Przeprowadzenie ogólnej analizy wymagane jest w szczególności przed:
   1) rozpoczęciem przetwarzania Danych,
   2) w przypadku istotnych zmian w procesie przetwarzania Danych,
   3) w związku okresowymi przeglądami wykonywanymi przez Administratora,
   4) w związku z zgłoszonymi zasadnymi naruszeniami ochrony Danych Osobowych.
5. Na Administratorze spoczywa odpowiedzialność w zakresie:
   1) wyboru metody prowadzenia analizy ryzyka, np. ilościowa, jakościowa, mieszana,
   2) wyboru narzędzi prowadzenia analizy ryzyka, np. ankiety, kwestionariusze, scenariusze, macierze,
   3) zaangażowaniu wymaganych podmiotów i osób z wewnątrz albo z zewnątrz organizacji,
   4) doboru możliwych do zastosowania środków obniżających ryzyko związane z przetwarzaniem Danych.
6. Ocena procesu przetwarzania w ramach ogólnej analizy ryzyka powinna być obiektywna, Administrator zobowiązany jest stwierdzić, czy z operacjami przetwarzania Danych wiąże się ryzyko lub wysokie ryzyko – skala oceny powinna zawierać minimum dwa poziomy oceny.

§21

Wewnętrzne regulacje (polityki)

1. Obowiązkiem Administratora jest opracowanie i przyjęcie do stosowania sformalizowanych wewnętrznych regulacji (polityk) opisujących posiadane środki techniczne i organizacyjne zapewniające zgodność przetwarzania z RODO.

2. Zakres i sposób opracowania wewnętrznych regulacji (polityk), o których mowa w ust. 1, powinien być adekwatny do skali prowadzonej działalności Administratora oraz wyników analizy ryzyka przetwarzania.
3. Przykładowy wykaz obszarów przetwarzania Danych, których opracowanie i wdrożenie powinien rozważyć Administrator stanowi Załącznik nr 4 do Kodeksu.
4. Obowiązkiem Administratora jest wykonywanie okresowych przeglądów i w razie potrzeby aktualizacji wewnętrznych regulacji (polityk).

VII Zasady przetwarzania Danych i środki stosowane przy przetwarzaniu

§22

Uwzględnienie ochrony Danych w fazie projektowania oraz domyślna ochrona Danych

1. W przypadku gdy opracowywane, projektowane, wybierane lub użytkowane są aplikacje, systemy informatyczne, usługi i produkty obejmujące przetwarzanie Danych Osobowych, Administrator podczas ich projektowania powinien wziąć po uwagę prawo do ochrony prywatności i, uwzględniając poziom ryzyka naruszenia praw i wolności osób fizycznych, a także stan wiedzy technicznej, wdrożyć odpowiednie środki techniczne i organizacyjne.
2. Decyzja Administratora o zastosowanych środkach organizacyjnych i technicznych, jak również wymaganiach funkcjonalnych jest każdorazowo uzależniona od charakteru, zakresu, kontekstu i celów przetwarzania Danych oraz od stanu aktualnej wiedzy technicznej i przewidywanych kosztów wdrożenia odpowiednich zabezpieczeń.
3. Środkami mającymi na celu zapewnienie ochrony Danych są np. pseudonimizacja czy minimalizacja Danych, integracja niezbędnych zabezpieczeń, a także stosowanie zasad: prawidłowości Danych, ograniczenia celu przetwarzania, przejrzystości przetwarzania oraz ograniczenia przetwarzania.
4. Podstawowe zasady w domyślnej ochronie Danych obejmują przetwarzanie Danych, które są niezbędne do osiągnięcia każdego, konkretnego celu przetwarzania i w szczególności obejmują takie elementy, jak:
   1) ilość zbieranych Danych Osobowych,
   2) zakres przetwarzania Danych,
   3) okres przechowywania Danych,
   4) dostępność (Danych dla innych osób).
5. W niniejszym Kodeksie przedstawione zostały podstawowe funkcjonalności oraz wymagania techniczne, których zastosowanie pozwoli na ograniczenie ryzyka naruszenia praw lub wolności osób fizycznych, których Dane są przetwarzane. Propozycje zabezpieczeń zostały wskazane w Załączniku nr 7.
6. Administrator może wywiązać się z obowiązków w zakresie stosowania zasad ochrony Danych w fazie projektowania oraz domyślnej ochrony Danych między innymi poprzez wprowadzenie zatwierdzonego mechanizmu certyfikacji określonego w art. 42 RODO.

§23

Przykładowe wymagania funkcjonalne systemów informatycznych przetwarzających Dane Osobowe

1. **Zbieranie Danych:**
   1) Zakres Danych zbieranych i utrzymywanych w systemie informatycznym powinien być ograniczony tylko do tych Danych, których zbieranie oparte jest na co najmniej jednym z warunków wskazanych w art. 6 RODO.
   2) W przypadku gdy Zgoda Podmiotu Danych będzie mogła być wyrażona w systemie informatycznym – system ten powinien spełniać poniższe warunki:
      a) system powinien umożliwiać równie łatwe udzielenie jak i odwołanie Zgody, które powinno skutkować zaprzestaniem przetwarzania Danych zebranych w określonych celach;
      b) Zgoda nie może być zaznaczona domyślnie;
      c) Zgoda powinna być wyrażona dobrowolnie, czyli od jej wyrażenia nie może być uzależniona np. realizacja umowy;
      d) fakt wyrażenia / cofnięcia Zgody powinien być odnotowany w systemie informatycznym w sposób zapewniający rozliczalność, w tym poprzez odnotowanie takich danych jak np. Dane osoby, data i treść Zgody. Jeżeli do przetwarzania Danych wykorzystywanych jest kilka systemów informatycznych, wystarczające jest odnotowanie Zgody przynajmniej w jednym systemie.

3) System informatyczny, jeżeli posiada taką funkcjonalność, powinien umożliwiać realizację praw Podmiotu Danych, na przykład w formie odrębnej informacji, jak również przewidywać klauzule informacyjne zgodne z zakresem i celem przetwarzanych Danych Osobowych.

2. **Zakończenie lub ograniczenie przetwarzania:**
   1) System informatyczny powinien umożliwiać zakończenie przetwarzania Danych po upływie oznaczonego okresu. W zależności od dostępnej funkcjonalności systemu, zakończenie przetwarzania może być zrealizowane poprzez usunięcie lub anonimizację Danych.
   2) System informatyczny, w zależności od dostępnej funkcjonalności, powinien umożliwiać realizację praw podmiotów Danych, zgodnie z Rozdziałem V Kodeksu.
   3) Żadna z powyższych operacji nie może zakłócać integralności Danych w systemach informatycznych.
3. **Jakość danych:**
   1) System informatyczny powinien zapewnić mechanizmy pozwalające na uaktualniane lub sprostowanie Danych (np. w przypadku zmiany Danych).
   2) Zaleca się, aby systemy informatyczne wyposażone były w mechanizmy walidujące lub weryfikujące poprawność wprowadzanych Danych (np. algorytmy sprawdzające sumę kontrolną numeru PESEL).
4. **Domyślna ochrona Danych („privacy by default"):**
   1) Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzane były wyłącznie te Dane Osobowe, które są niezbędne dla osiągniecia celów przetwarzania.
   2) Obowiązek odnosi się do ilości zbieranych Danych Osobowych, zakresu ich przewarzania, okresu ich przechowywania oraz ich dostępności (dla innych osób). W szczególności podejmowane środki mają na celu zapewnienie, by domyślnie Dane Osobowe nie były udostępniane bez interwencji Podmiotu Danych nieokreślonej liczbie osób.
   3) W praktyce oznacza to, że domyślne ustawienia programu (systemu), w przypadku systemów informatycznych udostępnianych Podmiotom Danych, powinny zawierać minimalny zakres Danych Osobowych, niezbędny do realizacji celów dla których zostały zebrane. Ustawienia te powinny być zdefiniowane domyślnie, czyli bez konieczności dodatkowej aktywności Podmiotów Danych.
5. Ochrona prywatności powinna być realizowana jako domyślne ustawienie każdego programu (systemu), a zmiana takiego ustawienia powinna być realizowana na wyraźne żądanie użytkownika programu.
6. **Zabezpieczenie danych:**
   1) W celu dodatkowego zabezpieczenia Danych, w tym zapewnienia ich dostępności powinien być stosowany mechanizm wykonywania kopii zapasowych. Częstotliwość i tryb wykonywania kopii zapasowych (kopie przyrostowe lub całościowe) może być uzależniony od zastosowanych mechanizmów bezpieczeństwa infrastruktury oraz ryzyka związanego z utratą Danych.
   2) Kopie zapasowe przechowywane są przez Administratora zgodnie z przyjętym okresem retencji Danych Osobowych, od chwili sporządzenia nośnika lub przez okres, który pozwala na prawidłowe odtworzenie Danych. W przypadku konieczności anonimizacji lub usuwania Danych znajdujących się na kopii zapasowej, niszczony jest cały nośnik lub usuwane (nadpisywane) Dane na nośniku w momencie upływu terminów, o których mowa w zdaniu poprzednim.

VIII Naruszenia ochrony Danych Osobowych

§24

Podejście do naruszeń ochrony Danych Osobowych

1. IZFiA opracowując podejście do naruszeń ochrony Danych Osobowych opiera swoje doświadczenia nie tylko na wymaganiach RODO, ale także najlepszych standardach oraz dobrych praktykach i wytycznych z zakresu zarządzania incydentami w bezpieczeństwie informacji, środowisku teleinformatycznym, a także technologii informacyjnej i ciągłości działania obowiązujących na rynku Funduszy Inwestycyjnych.
2. Podejście, na którym oparte jest zarządzanie naruszeniami ochrony Danych Osobowych wśród członków IZFiA wynika z najlepszych praktyk wypracowanych na przykład na bazie Opinii Grupy Roboczej Art. 29, standardu ISO/IEC 27001:2013 oraz Wytycznych dotyczących zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w sektorze finansowym i kapitałowym opracowanych przez Komisję Nadzoru Finansowego.
3. W przypadku wystąpienia naruszenia ochrony Danych Osobowych, Administrator formalnie dokumentuje fakt naruszenia Danych, wszelkie okoliczności tego naruszenia, jego ocenę, skutki oraz podjęte działania zaradcze.

§25

Zgłaszanie naruszenia ochrony Danych Osobowych organowi nadzorczemu

1. Podmioty Stosujące Kodeks posiadają sformalizowane zasady zarządzania incydentami naruszenia bezpieczeństwa informacji i Danych. Jednakże nie każdy incydent podlega obowiązkowemu zgłoszeniu do organu nadzorczego (notyfikacji) przez Administratora jako naruszenie ochrony Danych Osobowych.
2. Administrator jest zobowiązany do notyfikacji naruszenia tylko wówczas, gdy incydent naruszenia bezpieczeństwa informacji lub Danych spełnia łącznie dwie przesłanki, tj.:
    1) stanowi naruszenie ochrony Danych Osobowych – którym jest naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do Danych Osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
    2) skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych, z zastrzeżeniem ust. 10 i 11 poniżej.
3. Ocena naruszenia ochrony Danych może być analizowana między innymi z uwzględnieniem kontekstu przetwarzania Danych, łatwości identyfikacji Podmiotu Danych oraz okoliczności naruszenia, przy czym każdy z Podmiotów Stosujących Kodeks może opracować odrębną metodykę do analizy poziomu ryzyka naruszenia praw lub wolności osób fizycznych, zgodnie z zasadą rozliczalności.
5. Zgłoszenie naruszenia ochrony Danych Osobowych jest przekazywane przez Administratora do organu nadzorczego bez zbędnej zwłoki, jednak w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. Do zgłoszeń przekazywanych po upływie 72 godzin Administrator dołącza wyjaśnienie przyczyn opóźnienia.
6. Zgłoszenie naruszenia ochrony Danych Osobowych przekazywane do organu nadzorczego zawiera co najmniej informacje wskazane w Załączniku nr 5 do Kodeksu, zgodnie z art. 33 ust. 3 RODO. Zgłoszenie zawiera opis charakteru naruszenia na dzień jego sporządzenia i w razie pojawienia się nowych okoliczności w sprawie, mających istotny wpływ na opisany wcześniej charakter naruszenia, zgłoszenie może być zaktualizowane.
7. Zgłoszenie może być realizowane w formie pisemnej poprzez wysłanie powiadomienia na adres korespondencyjny organu nadzorczego lub w formie elektronicznej poprzez formularz udostępniony na oficjalnej stronie internetowej organu nadzorczego. Organ nadzorczy może doprecyzować sposób i zakres zgłaszania naruszeń ochrony Danych Osobowych.
8. Za naruszenie ochrony Danych Osobowych, które wymaga notyfikacji może być uznane w szczególności:
    1) utrata poufności lub integralności Danych Osobowych uniemożliwiająca wykonywanie obowiązków Administratora lub Podmiotu Przetwarzającego;
    2) wyciek bazy danych zawierającej informacje identyfikujące osobę i umożliwiające przejęcie jej tożsamości lub wykonanie transakcji (powiązanie takich danych jak, np.: imię i nazwisko, adres zameldowania, dane teleadresowe, numer PESEL, numer telefonu, adres konta poczty elektronicznej, dane dokumentu tożsamości, które umożliwi zidentyfikowanie osoby fizycznej);
    3) wyciek bazy zawierającej dane lub narzędzia służące do uwierzytelniania transakcji płatniczych lub korzystania z elektronicznych kanałów dostępu;
    4) wysłanie korespondencji zawierającej Dane Osobowe chronione tajemnicą zawodową do osoby nieuprawnionej (w formie papierowej lub elektronicznej);
    5) kradzież lub zagubienie dokumentów papierowych zawierających Dane Osobowe;
    6) kradzież lub zagubienie urządzeń przenośnych, mobilnych oraz elektronicznych nośników danych (np. laptopów, tabletów, smartfonów, pendrive'ów) zawierających niezabezpieczone (poprzez kryptograficzne środki ochrony, np. szyfrowanie) Dane Osobowe.
9. Naruszenie ochrony Danych Osobowych nie wymaga notyfikacji, jeżeli jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
10. Za naruszenie ochrony Danych Osobowych, które nie wymaga notyfikacji może być uznane w szczególności:
    1) wyciek danych, które nie umożliwiają identyfikacji osoby fizycznej, przejęcia jej tożsamości lub wykonania transakcji (np. baza danych po pseudonimizacji lub część bazy zawierająca tylko nazwy ulic, nazwy miast lub kody pocztowe);
    2) wyciek Danych zabezpieczonych z zastosowaniem środków kryptograficznej ochrony (np. z wykorzystaniem szyfrowania lub pseudonimizacji), z zastrzeżeniem, że nie doszło do jednoczesnego skompromitowania kluczy kryptograficznych używanych do ochrony Danych (np. klucza PGP);
    3) wyciek Danych lub narzędzia służącego do uwierzytelniania transakcji płatniczych lub korzystania z elektronicznych kanałów dostępu zabezpieczonych z zastosowaniem kryptograficznych środków ochrony (np. z wykorzystaniem szyfrowania lub pseudonimizacji), z zastrzeżeniem, że nie doszło do jednoczesnego skompromitowania kluczy kryptograficznych używanych do ochrony Danych (np. klucza PGP);

4) wysłanie Danych objętych tajemnicą zawodową w korespondencji elektronicznej do osoby nieuprawnionej z zastosowaniem kryptograficznych środków ochrony (zaszyfrowanych, zahasłowanych) bez jednoczesnego dostępu do narzędzi deszyfrujących i haseł;
5) kradzież lub zagubienie urządzeń przenośnych, mobilnych oraz elektronicznych nośników danych zawierających Dane Osobowe zabezpieczonych z zastosowaniem organizacyjnych, technicznych lub kryptograficznych środków ochrony (np. szyfrowanie, bezpieczne hasła, możliwość zdalnego czyszczenia danych z urządzenia mobilnego);
6) wyciek danych chronionych tajemnicą zawodową, które nie stanowią Danych Osobowych;
7) naruszenie integralności danych, jeżeli w wyniku błędnego wprowadzenia np. danych kontaktowych do systemu nie doszło do ujawnienia danych objętych Tajemnicą zawodowa lub praw i wolności Podmiotów Danych;
8) ujawnienie informacji prawnie chronionych osobie trzeciej, jeśli do ich ujawnienia doszło z winy Podmiotu Danych, w tym udostępnienie danych do logowania, umożliwienie zapoznania się z wiadomościami z poczty elektronicznej lub wiadomościami sms.

11. W celu zapewnienia rozliczalności Podmioty Stosujące Kodeks mogą prowadzić rejestr wszystkich incydentów bezpieczeństwa informacji i naruszeń ochrony Danych Osobowych.

§26

Zawiadamianie Podmiotu Danych, o naruszeniu ochrony Danych Osobowych

1. Niezależnie od obowiązków wskazanych w § 25 powyżej, Administrator jest zobowiązany do poinformowania Podmiotu Danych o naruszeniu ochrony jego Danych, w przypadku gdy incydent naruszenia bezpieczeństwa informacji lub Danych łącznie spełnia dwie przesłanki:
   1) stanowi naruszenie ochrony Danych Osobowych – przez co rozumie się takie naruszenie bezpieczeństwa, które prowadzi do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do Danych Osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
   2) skutkuje wysokim ryzykiem naruszenia praw lub wolności osób fizycznych – przez co rozumie się takie naruszenie bezpieczeństwa, które może powodować powstanie u osoby m.in.:
      a) uszczerbku fizycznego,
      b) szkód majątkowych lub niemajątkowych, takich jak: utrata kontroli nad własnymi Danymi lub ograniczenie praw, dyskryminacja, kradzież lub sfałszowanie tożsamości,
      c) nieuprawnionego odwrócenia pseudonimizacji,
      d) naruszenia dobrego imienia,
      e) naruszenia poufności Danych Osobowych chronionych tajemnicą zawodową.
2. Ocena naruszenia ochrony Danych jest analizowana w sposób opisany w § 25 ust. 3.
3. Zawiadomienie Podmiotu Danych o naruszeniu ochrony Danych może być uzależnione od współpracy Administratora z organem nadzorczym, z uwzględnieniem wskazówek lub wytycznych przekazanych przez ten organ lub inne organy państwowe, w tym organy ścigania.
4. Termin zawiadomienia Podmiotu Danych o naruszeniu ochrony Danych Osobowych może być uzależniony od charakteru i wagi naruszenia ochrony Danych Osobowych, jego konsekwencji oraz niekorzystnych skutków dla Podmiotu Danych, jednakże Administrator dokona zawiadomienia bez zbędnej zwłoki (w miarę możliwości nie później niż w terminie 30 dni po stwierdzeniu naruszenia). Przykładowo, potrzeba zminimalizowania bezpośredniego ryzyka wystąpienia szkody Podmiotu Danych będzie uzasadniała niezwłoczne jej poinformowanie, natomiast wdrożenie przez Administratora odpowiednich środków bezpieczeństwa przeciwko takim samym lub podobnym naruszeniom w przyszłości będzie uzasadniała późniejszą realizację obowiązku informacyjnego.
5. Zawiadomienie Podmiotu Danych zawiera co najmniej informacje wskazane w Załączniku nr 6 do Kodeksu, zgodnie z art. 34 ust. 2 RODO. Zawiadomienie zawiera opis charakteru naruszenia na dzień jego sporządzenia.
6. Z zastrzeżeniem dokonania oceny ryzyka naruszenia, za naruszenie ochrony Danych Osobowych, które wymaga zawiadomienia Podmiotu Danych, mogą być uznane w szczególności przypadki wymienione w § 25 ust. 9.
7. Zawiadomienie może być realizowane z wykorzystaniem kanałów zapewniających bezpieczne przekazywanie korespondencji, w tym w szczególności w formie pisemnej na adres korespondencyjny lub elektronicznie przy wykorzystaniu dostępnych u Administratora technologii oraz kanałów komunikacji.
8. Zawiadomienie Podmiotu Danych o naruszeniu ochrony Danych Osobowych nie jest wymagane w następujących przypadkach:
   1) Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do Danych Osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie lub inne środki opisane w Załączniku nr 6, uniemożliwiające odczyt osobom nieuprawnionym oraz dostęp do tych Danych;

2) Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności Podmiotu Danych, w tym poprzez zastosowanie odpowiednich technicznych i organizacyjnych środków ochrony;
3) wymagałoby ono niewspółmiernie wysokiego wysiłku - w takim przypadku wydawany jest publiczny komunikat, w szczególności w postaci informacji na stronie WWW Administratora lub zastosowany zostaje podobny środek, za pomocą którego Podmioty Danych, zostają poinformowane w równie skuteczny sposób.

9. Za naruszenie ochrony Danych Osobowych, które nie wymaga zawiadomienia Podmiotu Danych mogą być uznane w szczególności przypadki wskazane w § 25 ust. 11.
10. Zawiadomienie Podmiotu Danych o naruszeniu ochrony Danych Osobowych może zostać zrealizowane w późniejszym terminie niż wskazany w ust. 4 lub Administrator może odstąpić od takiego zawiadomienia w szczególności, jeżeli:
    1) zawiadomienie będzie stanowiło naruszenie przepisów powszechnie obowiązującego prawa lub obowiązku ochrony Danych Osobowych innych Podmiotów Danych;
    2) przepisy powszechnie obowiązującego prawa przewidują inny, określony w nich termin zawiadomienia Podmiotu Danych o takim naruszeniu.

IX Podmiot Przetwarzający

§27

1. Administrator może korzystać z usług Podmiotów Przetwarzających, posiadających wiedzę fachową, wiarygodność i zasoby, które zapewnią wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, w zakresie przetwarzania zleconym przez Administratora. Za gwarancję wdrożenia odpowiednich środków technicznych i organizacyjnych, o których mowa powyżej, mogą być uznane w szczególności:
    a) stosowanie przez Podmiot Przetwarzający zatwierdzonego kodeksu RODO,
    b) stosowanie przez Podmiot Przetwarzający mechanizmu certyfikacji opisanego w art. 42 RODO,
    c) posiadanie aktualnej certyfikacji na zgodność z normą ISO 27001 lub udokumentowanego innego audytu w tym obszarze np. ISAE 3000 lub 3402,
    d) świadczenie na rzecz Administratora usług, które wymagają zezwolenia Komisji Nadzoru Finansowego.
2. Administrator przed powierzeniem przetwarzania Danych Osobowych bierze pod uwagę standardy bezpieczeństwa stosowane przez Podmiot Przetwarzający lub wyznacza wymagany przez Administratora standard w tym zakresie (np. za pomocą audytu lub ankiety), z zastrzeżeniem ust. 1 pkt a)-c).
3. Przekazanie Danych do przetwarzania przez Podmiot Przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, np. jednostronnej czynności prawnej Administratora, zgodnych w szczególności z art. 28 RODO. Podmiot Przetwarzający przetwarza Dane w zakresie wskazanym umową lub innym instrumentem prawnym.
4. Podmiot Przetwarzający może powierzyć przetwarzanie Danych innemu podmiotowi wyłącznie po uzyskaniu zgody Administratora. Takie powierzenie odbywa się zgodnie z postanowieniami ust. 1 i 2.
5. Podmiot Przetwarzający, po rozwiązaniu umowy z Administratorem, zgodnie z decyzją Administratora powinien zwrócić lub usunąć Dane oraz usunąć wszelkie ich istniejące kopie, a w razie braku decyzji usunąć te Dane oraz wszelkie ich istniejące kopie, chyba że istnieje inna podstawa przetwarzania (np. do celu ewentualnego dochodzenia roszczeń).

X Rejestrowanie czynności przetwarzania

§28

1. Każdy Administrator prowadzi rejestr czynności przetwarzania Danych Osobowych. Rejestr prowadzony jest przez Towarzystwo Funduszy Inwestycyjnych dla wszystkich zarządzanych Funduszy Inwestycyjnych.
2. W rejestrze czynności przetwarzania Danych Osobowych zamieszcza się wszystkie następujące informacje:
    a) nazwę oraz dane kontaktowe Administratora oraz wszelkich współadministratorów, a także inspektora ochrony danych;
    b) cele przetwarzania;
    c) opis kategorii Podmiotów Danych, oraz kategorii Danych Osobowych;
    d) kategorie Odbiorców, którym Dane Osobowe zostały lub zostaną ujawnione, w tym Odbiorców w państwach trzecich lub w organizacjach międzynarodowych;

e) gdy ma to zastosowanie – fakt przekazania Danych Osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwę tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentację odpowiednich zabezpieczeń;
f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii Danych;
g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

3. Każdy Podmiot Przetwarzający prowadzi rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora. W rejestrze tym zamieszcza się wszystkie następujące informacje:
   a) nazwę oraz dane kontaktowe Podmiotu Przetwarzającego lub Podmiotów Przetwarzających oraz każdego Administratora, w imieniu którego działa Podmiot Przetwarzający oraz inspektora ochrony danych. W przypadku Podmiotu Przetwarzającego rejestr prowadzony jest w podziale na Towarzystwa Funduszy Inwestycyjnych.
   b) kategorie przetwarzań dokonywanych w imieniu każdego z Administratorów;
   c) gdy ma to zastosowanie – fakt przekazania Danych Osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwę tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentację odpowiednich zabezpieczeń;
   d) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.
4. Rejestry, o których mowa w ust. 1 i 2, mają formę pisemną, w tym dopuszczalna jest forma elektroniczna. Rejestr zostanie udostępniony na żądanie Prezesa Urzędu Ochrony Danych Osobowych.
5. Uznaje się, że wyłączenia z obowiązku prowadzenia rejestru czynności przetwarzania i rejestru wszystkich kategorii czynności przetwarzania na podstawie art. 30 ust. 5 RODO nie stosuje się wobec Podmiotów Stosujących Kodeks.

XI Bezpieczeństwo przetwarzania

§29

1. Administrator oraz Podmiot Przetwarzający Dane Osobowe zobowiązany jest do wdrożenia mechanizmów ochrony Danych Osobowych zgodnie ze stanem wiedzy technicznej, kosztem wdrożenia zabezpieczeń oraz charakterem, zakresem, kontekstem i celami przetwarzania, z jednoczesnym uwzględnieniem ryzyka naruszenia praw lub wolności Podmiotu Danych.
2. Uznaje się, że Podmioty Stosujące Kodeks wywiązują się z obowiązku wdrożenia odpowiednich środków technicznych i organizacyjnych oraz zapewniają bezpieczeństwo Danych Osobowych, w przypadkach gdy:
   1) posiadają certyfikat lub znak jakości, o którym mowa w art. 42 RODO, lub
   2) stosują niniejszy Kodeks postępowania, lub
   3) posiadają aktualną certyfikację na zgodność z normą ISO 27001 lub udokumentowany audyt ISAE 3000 lub 3402.
3. Środki bezpieczeństwa technicznego i organizacyjnego opisane w Załączniku nr 7 do Kodeksu postępowania nie wyczerpują możliwych zabezpieczeń stosowanych przez Administratora oraz Podmiot Przetwarzający. Podmioty Stosujące Kodeks w celu podnoszenia świadomości i kultury bezpieczeństwa oraz zapewnienia dodatkowych mechanizmów ochrony Danych mogą korzystać z najlepszych praktyk i standardów, w tym w szczególności:
   1) praktyk wypracowanych na bazie Opinii Grupy Roboczej Art. 29;
   2) standardów systemu zarządzania bezpieczeństwem informacji z grupy ISO 27000, w tym ISO/IEC 27001:2013;
   3) Wytycznych dotyczących zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w sektorze finansowym i kapitałowym opracowanych przez Komisję Nadzoru Finansowego;
   4) udokumentowanego audytu ISAE 3000 lub 3402.
4. W celu zapewnienia odpowiednej jakości wdrożonych środków bezpieczeństwa technicznego i organizacyjnego Administrator lub Podmiot Przetwarzający zapewnia regularne testowanie tych środków. W przypadku stosowania certyfikacji lub znaku jakości, o których mowa w ust. 2 pkt 1) lub certyfikatu ISO 27000, o którym mowa w ust. 3 pkt 2) lub audyt ISAE o którym mowa w ust. 3 pkt 4) uznaje się, że regularne sprawdzenie jest realizowane.

XII Przeprowadzenie oceny skutków dla ochrony Danych Osobowych

§30

1. Administrator powinien przed rozpoczęciem przetwarzania rozważyć przeprowadzenie szczegółowej oceny ryzyka, tj. oceny skutków dla ochrony Danych osobowych w rozumieniu RODO, przykładowo w następujących sytuacjach:
   a) przed wykorzystaniem nowych technologii przetwarzania Danych, takich jak np. nowych systemów informatycznych, wprowadzania istotnych modyfikacji do istniejących systemów,
   b) przed wprowadzeniem nowej usługi lub nowego typu produktu,
   c) przejęcie Danych od innych Administratorów np. w związku połączeniem Funduszy Inwestycyjnych,

   pod warunkiem, że przetwarzanie ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych
2. Administrator jest obowiązany również wykonać ocenę skutków dla ochrony Danych gdy dany rodzaj przetwarzania został określony w art. 35 ust. 3 RODO lub dany rodzaj przetwarzania został wskazany w wykazie podanym do publicznej wiadomości przez organ nadzorczy, zgodnie z art. 35 ust. 4 RODO.
3. Dla podobnych operacji przetwarzania Danych wiążących się z podobnym ryzykiem można przeprowadzić pojedynczą ocenę skutków dla ochrony Danych.
4. W przypadku, w którym ocena skutków dla ochrony Danych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, którego Administrator nie może zminimalizować poprzez zastosowanie odpowiednich środków, przed przetwarzaniem Administrator zobowiązany jest do skonsultowania się z organem nadzorczym.

XIII Przechowywanie i usuwanie Danych

§31

Zasady przechowywania i usuwania Danych

1. Dane Osobowe nie mogą być przechowywane w formie umożliwiającej ich identyfikację przez okres dłuższy, niż jest to niezbędne do realizacji celów, w których Dane zostały zebrane. Wskazanie okresu retencji Danych może mieć charakter opisowy umożliwiający w każdym przypadku indywidualne ustalenie jego długości.
2. Po osiągnięciu zamierzonych celów przetwarzania Dane Osobowe Podmiotów Danych powinny zostać usunięte lub zanonimizowane, chyba że ich dalsze przechowywanie znajduje podstawę prawną.
3. Dalsze przechowywanie Danych Osobowych jest dopuszczalne w przypadku ich przetwarzania m.in. w celu:
   1) archiwalnym dla zabezpieczenia się przed roszczeniami do czasu ich przedawnienia w związku ze świadczoną usługą - Dane usuwamy po zakończeniu roku, w którym przedawniło się roszczenie,
   2) ciągłego i niezakłóconego prowadzenia działalności poprzez zapewnienie integralności kopii archiwalnych lub awaryjnych od momentu ich utworzenia aż do likwidacji,
   3) realizacji zadań przez instytucje obowiązane w związku z przeciwdziałaniem praniu pieniędzy oraz finansowaniu terroryzmu,
   4) realizacji przepisów dotyczących implementacji MIFID.
4. Administrator może przechowywać Ddane przez okres dłuższy niż wskazany w ust. 2 o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, celów badań naukowych lub historycznych lub do celów statystycznych z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne (patrz Załącznik nr 7) w celu ochrony praw i wolności Podmiotów Danych .
5. Administrator powinien ustalić termin zanonimizowania/usuwania lub okresowego przeglądu Danych Osobowych, aby zapobiec przechowywaniu tych Danych Osobowych przez okres dłuższy niż jest to niezbędne.
6. Usunięcie Danych Osobowych Podmiotów Danych może być realizowane w szczególności poprzez ich zniszczenie lub anonimizację.

XIV Załączniki

1. Załącznik nr 1 – Przykładowy wzór klauzuli Zgody
2. Załącznik nr 2 – Przykładowy wzór klauzuli informacyjnej
3. Załącznik nr 3 – Zakres Danych podlegających przenoszeniu
4. Załącznik nr 4 – Wykaz wewnętrznych regulacji (polityk) w ramach procesu przetwarzania Danych
5. Załącznik nr 5 – Wzór powiadomienia o naruszeniu ochrony Danych Osobowych – zgłoszenie do organu nadzorczego
6. Załącznik nr 6 – Wzór powiadomienia o naruszeniu ochrony Danych Osobowych – zawiadomienie Podmiotu Danych
7. Załącznik nr 7 – Proponowane środki zabezpieczeń organizacyjnych i technicznych

Załącznik nr 1
do Kodeksu postępowania IZFiA

KLAUZULE ZGODY

1. Zgoda na przesyłanie informacji handlowych wybranymi kanałami komunikacji

Wyrażam zgodę na otrzymywanie informacji handlowych, w tym marketingu bezpośredniego, wysyłanych przez [*nazwa*] („Administrator") z siedzibą w […], ul. […] , […]-[…] [*miasto*], dotyczących usług i produktów Administratora**,** jak również podmiotów z grupy kapitałowej do której należy Administrator lub innych podmiotów, których aktualna lista znajduje się pod adresem [*adres strony internetowej*] za pośrednictwem[1]:

☐ adresu e-mail,

☐ numeru telefonu (w tym automatycznych systemów wywołujących).

Oświadczam również, że zostałem poinformowany, że:

1) administratorem moich danych osobowych jest [*nazwa*] („Administrator") z siedzibą w […], ul. […], […]-[…] [*miasto*],
2) dane kontaktowe inspektora ochrony danych: [*adres e-mail*],
3) moje dane osobowe przetwarzane będą w celu otrzymywania informacji handlowych w objętych zgodą kanałach, na podstawie art. 6 ust. 1 lit. a Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE („Ogólne Rozporządzenie o Ochronie Danych"),
4) odbiorcami moich danych osobowych mogą być w szczególności: agent transferowy prowadzący rejestr uczestników lub podmiot prowadzący ewidencję uczestników funduszy inwestycyjnych zarządzanych przez towarzystwo, depozytariusz, dystrybutorzy jednostek uczestnictwa, podmioty świadczące usługi doradcze i audytowe, informatyczne, archiwizacji i niszczenia dokumentów oraz usługi marketingowe na rzecz funduszy inwestycyjnych lub towarzystwa, biegli rewidenci w związku z audytem,
5) moje dane osobowe będą przechowywane przez okres niezbędny do przekazywania informacji handlowych nie dłużej niż do momentu cofnięcia zgody lub wyrażenia sprzeciwu na przetwarzanie w celu marketingu bezpośredniego,
6) posiadam prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przeniesienia danych,
7) mam możliwość wycofania zgody na każdy z kanałów komunikacji, a wycofanie zgody nie wpływa na zgodność z prawem przetwarzania danych osobowych, którego dokonano na podstawie zgody przed jej wycofaniem,
8) mam prawo wniesienia sprzeciwu wobec przetwarzania moich danych osobowych do celu marketingu bezpośredniego, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z marketingiem bezpośrednim,
9) przysługuje mi uprawnienie wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych,
10) wyrażenie zgody na kontaktowanie się ze mną każdym z kanałów komunikacji jest dobrowolne.

[1] Prosimy zaznaczyć „x" w okienkach, które odpowiadają kanałom komunikacji/sposobom za pomocą których zgadza się Pani/Pan na kontaktowanie się z Panią/Panem przez Administratora.

Załącznik nr 2
do Kodeksu postępowania IZFiA

KLAUZULA INFORMACYJNA

Niniejszym oświadczam, że zostałem poinformowany, że:

1) administratorem moich danych osobowych jest fundusz [*nazwa*]/są fundusze [*nazwy*] („Fundusz"/„Fundusze") z siedzibą w […], ul. […], […]-[…] [*miasto*], [*numer telefonu lub adres poczty elektronicznej*], w imieniu których działa i którymi zarządza [*nazwa*] Towarzystwo Funduszy Inwestycyjnych S.A. („Towarzystwo") z siedzibą w […], ul. […], […]-[…] [*miasto*],
2) dane kontaktowe inspektora ochrony danych: [*adres e-mail lub telefon*],
3) moje dane osobowe przetwarzane będą, gdy jest to niezbędne do:
   a) wykonania umowy, na podstawie art. 6 ust. 1 lit. b Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE („Ogólne Rozporządzenie o Ochronie Danych"),
   b) wypełnienia obowiązków prawnych ciążących na administratorze danych osobowych, na podstawie art. 6 ust. 1 lit. c Ogólnego Rozporządzenia o Ochronie Danych Osobowych, wynikających z ustawy z dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi, ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu, ustawy z dnia 9 października 2015 r. o wykonywaniu Umowy między Rządem Rzeczpospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki w sprawie poprawy wypełniania międzynarodowych obowiązków podatkowych oraz wdrożenia ustawodawstwa FATCA oraz ustawy z dnia 9 marca 2017 r. o wymianie informacji podatkowych z innymi państwami (CRS),
   c) do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub stronę trzecią, na podstawie art. 6 ust. 1 lit. f Ogólnego Rozporządzenia o Ochronie Danych Osobowych, za które administrator uznaje w szczególności: marketing bezpośredni, dochodzenie i obronę przed roszczeniami, zapobieganie oszustwom, przesyłanie danych w ramach grupy przedsiębiorstw, prowadzenie statystyk i analiz, zapewnienie bezpieczeństwa środowiska teleinformatycznego, stosowanie systemów kontroli wewnętrznej,
4) odbiorcami moich danych osobowych mogą być w szczególności: agent transferowy prowadzący rejestr uczestników lub podmiot prowadzący ewidencję uczestników Funduszu /Funduszy, depozytariusz, dystrybutorzy jednostek uczestnictwa, podmioty świadczące usługi doradcze, audytowe, księgowe, informatyczne, archiwizacji i niszczenia dokumentów, marketingowe, jak również biegli rewidenci w związku z audytem,
5) moje dane osobowe będą przechowywane przez okres: niezbędny do wykonywania umowy, wypełniania obowiązków prawnych ciążących na administratorze, oraz dochodzenia i obrony przed roszczeniami przez okres wynikający z biegu ogólnych terminów przedawnienia roszczeń liczony od ustania uczestnictwa,
6) mam prawo wniesienia sprzeciwu wobec przetwarzania moich danych osobowych do celu marketingu bezpośredniego, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z marketingiem bezpośrednim,
7) mam prawo wniesienia sprzeciwu wobec przetwarzania moich danych osobowych gdy przetwarzanie jest niezbędne do pozostałych celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora, bez wpływu na zgodność z prawem przetwarzania,
8) posiadam prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przeniesienia danych,
9) przysługuje mi uprawnienie wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych,
10) podanie moich danych osobowych jest dobrowolne, jednak jest niezbędne do realizacji mojego uczestnictwa w Funduszu/Funduszach i brak ich podania uniemożliwi zawarcie umowy.

Załącznik nr 3
do Kodeksu postępowania IZFiA

KATALOG DANYCH PODLEGAJĄCYCH PRZENOSZENIU

Dążąc do transparentności realizacji prawa do przenoszenia Danych Administratorzy oraz Podmioty Przetwarzające jako podmioty prowadzące rejestry i ewidencje ustalają wspólny katalog Danych podlegających przenoszeniu. Administratorzy deklarują, że w wykonaniu prawa do przeniesienia będą udostępniać (wydawać bądź przesyłać) osobom uprawnionym, w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego następujące Dane zawarte w rejestrze bądź ewidencji uczestników:

DANE OSOBOWE PODLEGAJACE WYDANIU PODMIOTOWI DANYCH	
Dane Osobowe uczestnika w rejestrze/ewidencji uczestników	▪ IMIĘ I NAZWISKO ▪ NUMER PESEL ▪ DATA URODZENIA ▪ MIEJSCE / KRAJ URODZENIA ▪ OBYWATELSTWO ▪ DANE DOKUMENTU TOŻSAMOŚCI: DOWÓD-PASZPORT-INNY (seria i nr, kraj wydania, data wystawienia, data ważności) ▪ ADRES ZAMELDOWANIA Z KODEM POCZTOWYM ▪ ADRES ZAMIESZKANIA Z KODEM POCZTOWYM ▪ ADRES DO KORESPONDENCJI ▪ TEL.KONTAKTOWY ▪ REZYDENCJA PODATKOWA ▪ NR RACHUNKU BANKOWEGO
Historia transacji * **wydawana na prośbę uczestnika, standardowo dotyczy okresu 1 roku przed złożeniem żądania*	▪ Data zlecenia nabycia / odkupienia/konwersji/zamiany ▪ Nr rejestru ▪ Kwota ▪ Ilość jednostek uczestnictwa / certyfikatów
STOSOWANY FORMAT	
XLS, CSV, XML, HTML	

Załącznik nr 4
do Kodeksu postępowania IZFiA

Wykaz wewnętrznych regulacji (polityk) w ramach procesu przetwarzania Danych

Podmioty Stosujące Kodeks opracują i wdrożą wewnętrzne regulacje (polityki) w następujących obszarach:

1. Przetwarzanie Danych Osobowych, z uwzględnieniem w szczególności zasad przetwarzania Danych Osobowych, w tym zasady „privacy by design" oraz „privacy by default".
2. Prowadzenie Rejestru Czynności Przetwarzania, realizacji praw Podmiotów Danych.
3. Powierzanie przetwarzania Danych Osobowych.
4. Bezpieczeństwo Danych Osobowych, w tym zarządzanie ryzykiem naruszenia praw i wolności Podmiotów Danych.
5. Ocena skutków dla ochrony Danych Osobowych.
6. Inspektor Ochrony Danych.
7. Zgłaszanie naruszeń ochrony danych osobowych organowi nadzoru oraz Podmiotom Danych.

Załącznik nr 5
do Kodeksu postępowania IZFiA

WZÓR POWIADOMIENIA O NARUSZENIU OCHRONY DANYCH OSOBOWYCH –
ZGŁOSZENIE DO ORGANU NADZORCZEGO

Nazwa administratora danych (Administrator):
Dane kontaktowe inspektora ochrony danych: *[imię, nazwisko, dane kontaktowe, adres e-mail, numer telefonu]*
Data powiadomienia:

Zgłoszenie naruszenia ochrony danych osobowych:
1) działając na podstawie art. 33 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE („RODO"),
2) w związku ze stwierdzeniem naruszenia ochrony danych osobowych
Administrator niniejszym przekazuje następujące informacje.

Charakter naruszenia:

Data stwierdzenia naruszenia	
Opis charakteru naruszenia	
Kategoria osób, których dane zostały naruszone	
Przybliżona liczba osób, których dane zostały naruszone	
Kategorie wpisów danych osobowych, których dotyczy naruszenie	
Przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie	
Możliwe konsekwencje naruszenia ochrony danych osobowych	
Środki zastosowane przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych	
Środki proponowane przez Administratora w celu zminimalizowania ewentualnych negatywnych skutków naruszenia	

Zgłoszenie zawiera opis stanu faktycznego na dzień jego sporządzenia i w razie pojawienia się nowych okoliczności w sprawie, mających istotny wpływ na opisany powyżej charakter naruszenia, zgłoszenie może zostać zaktualizowane.

Jednocześnie, z uwagi na upływ 72 godzin od stwierdzenia naruszenia, Administrator wyjaśnia, iż przyczyną opóźnienia przekazania niniejszego zgłoszenia jest ……..[2]

Z poważaniem,
….

[2] Stosowane w przypadku opóźnienia w realizacji obowiązku zgłoszenia do organu nadzoru

Załącznik nr 6
do Kodeksu postępowania IZFiA

WZÓR POWIADOMIENIA O NARUSZENIU OCHRONY DANYCH OSOBOWYCH – ZAWIADOMIENIE OSOBY, KTÓREJ DANE DOTYCZĄ

Nazwa administratora danych (Administrator):
Dane kontaktowe inspektora ds. ochrony danych: *[imię, nazwisko, dane kontaktowe, adres e-mail, numer telefonu]*
Data powiadomienia:

Szanowna Pani/Szanowny Panie,

Administrator … z siedzibą w …, przy ul. … uprzejmie informuje o stwierdzeniu naruszenia ochrony Pani/Pana danych osobowych przetwarzanych przez Administratora w związku z … *[rodzaj świadczonej usługi, proces]*, które może powodować wysokie ryzyko naruszenia Pani/Pana praw lub wolności.

Poniżej przekazujemy informacje dotyczące charakteru naruszenia ochrony danych:

1. Naruszenie polegało na …
2. Możliwe są następujące konsekwencje naruszenia …
3. Administrator po stwierdzeniu naruszenia niezwłocznie podjął niezbędne środki w celu usunięcia/zminimalizowania ewentualnych skutków …

Administrator zapewnia, iż podjął niezbędne działania w celu zapobieżenia podobnym sytuacjom w przyszłości.

W razie dodatkowych pytań lub sugestii zapraszamy do kontaktu z Inspektorem ds. ochrony danych.

Niniejsze zawiadomienie zostało przygotowane przez Administratora zgodnie z wymaganiami art. 34 ust. 2 Ogólnego rozporządzenia o ochronie danych Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE („RODO") i zawiera opis stanu faktycznego na dzień sporządzenia zawiadomienia.

Dodatkowo informujemy, że zgodnie z art. 33 ust. 1 RODO, Administrator przekazał zawiadomienie o przedmiotowym naruszeniu do Prezesa Urzędu Ochrony Danych Osobowych.

Z poważaniem,
….

PROPONOWANE ŚRODKI ZABEZPIECZEŃ ORGANIZACYJNYCH	
Grupa zabezpieczeń	**Opis zabezpieczeń**
1. Środki organizacyjne	W procesie przetwarzania Danych Osobowych stosowane są w szczególności poniższe środki ochrony: 1. Powołano inspektora ochrony danych. 2. Opracowano i wdrożono polityki bezpieczeństwa oraz plan ciągłości działania. 3. Zapewniono kontrolę nad dostępem do Danych Osobowych. 4. Zapewniono szkolenia z zakresu bezpieczeństwa przetwarzania Danych dla osób biorących udział w procesie przetwarzania. 5. Zobowiązano osoby biorące udział w przetwarzaniu Danych do zachowania tajemnicy. 7. Prowadzony jest rejestr czynności przetwarzania Danych. 8. Prowadzony jest rejestr naruszeń ochrony Danych Osobowych. 9. Prowadzona jest analiza ryzyka oraz ocena skutków dla ochrony Danych.
ŚRODKI ZABEZPIECZEŃ TECHNICZNYCH	
Grupa zabezpieczeń	**Opis zabezpieczeń**
2. Środki ochrony fizycznej i środowiskowej	1. W celu zabezpieczenia budynków oraz pomieszczeń, w których przetwarzane są Dane osobowe stosowane są w szczególności poniższe środki ochrony: 1) Zapewnienie kontroli dostępu fizycznego do budynku oraz pomieszczeń w których przetwarzane są Dane Osobowe. 2) Zapewnienie bezpieczeństwa przeciwpożarowego. 3) Zapewnienie ochrony dokumentów oraz Danych przed dostępem osób postronnych oraz uszkodzeniem lub zniszczeniem. 4). Zapewnienie skutecznych metod niszczenia dokumentów i Danych.
3. Zabezpieczenia techniczne i systemów teleinformatycznych	W procesie przetwarzania Danych Osobowych wykorzystywane są w szczególności poniższe środki ochrony, które mogą się różnić w zależności od funkcjonalności poszczególnych systemów: 1. Zastosowanie w przypadku uznania za właściwą metodę ochrony mechanizmów szyfrowania Danych lub innych zabezpieczeń w tym pseudonimizacji: 1) za pseudonimizację uznaje się usunięcie z podstawowej bazy danych informacji mogących zidentyfikować osoby, których dane zgromadzone są w tej bazie danych. Informacje mogące zidentyfikować osoby przechowywane są w odrębnej bazie danych o ograniczonym dostępie, niemającej bezpośredniego połączenia z główną bazą danych, która została poddana pseudonimizacji; 2) za szyfrowanie uznaje się zabezpieczenie przesyłanych danych, baz danych oraz ich kopii zapasowych przed odczytem przez osoby nieuprawnione poprzez zastosowanie algorytmu szyfrującego. Odczyt rekordów z zaszyfrowanej bazy danych możliwy jest za pomocą klucza (hasła) umożliwiającego odszyfrowanie. Algorytm szyfrujący jak również klucz (hasło) służące do odszyfrowania zabezpieczone są przed nieuprawnionym ujawnieniem. 2. Zapewnienie poufności, integralności, rozliczalności, dostępności i odporności systemów: 1) W celu zapewnienia poufności stosuje się: a) unikalne identyfikatory użytkowników, b) złożone hasła dostępu, c) obowiązek okresowej zmiany haseł, d) zróżnicowane poziomy uprawnień, e) oprogramowanie antywirusowe lub inne oprogramowanie identyfikujące podejrzane aktywności w systemach lub na stacjach roboczych, f) kontrolę oraz monitorowanie styku sieci wewnętrznej z siecią Internet (zapory ogniowe, proxy),

	g) środki kryptograficznej ochrony na poziomie transmisji danych przesyłanych z wykorzystaniem sieci Internet, h) mechanizmy identyfikacji i uwierzytelniania użytkowników (co najmniej identyfikator i hasło) w przypadku udostępniania aplikacji dostępnych przez sieć Internet. 3. W celu zapewnienia dostępności i odporności stosuje się: 1) systemy zapewniające dostępność zgodnie z zakresem świadczonych usług, 2) systemy i rozwiązania do wykonywania kopii zapasowych, 3) systemy podtrzymania napięcia (UPS), 4) kontrolę ruchu w sieci wewnętrznej, 5) ograniczanie pojedynczych punktów awarii lub minimalizowanie ryzyka związanego z wykonywaniem awarii, 6) oprogramowanie antywirusowe i kontrolę dostępu do sieci Internet (np. proxy, antyspam), 7) sformalizowane zasady zgłaszania incydentów związanych z bezpieczeństwem systemów. 4. W celu zapewnienia integralności i rozliczalności stosuje się: 1) logowanie działalności użytkowników w szczególności w systemach krytycznych (repozytorium z logami), 2) logowanie wykonanych zmian na Danych Osobowych przez użytkowników, w szczególności w systemach krytycznych, 3) kontrolę jakości danych (w tym m.in. zastosowanie mechanizmów walidacyjnych, weryfikacji poprawności danych – np. maker-checker).
5.Środki ochrony w ramach narzędzi programowych i baz danych	W procesie przetwarzania Danych Osobowych wykorzystywane są w szczególności poniższe środki ochrony, które mogą się różnić w zależności od funkcjonalności poszczególnych narzędzi programowych i baz danych: 1. stosowanie mechanizmów bazodanowych zapewniających integralność danych o ile wykorzystanie takich mechanizmów jest uzasadnione ze względu na ilość przetwarzanych Danych, 2. Kontrolę nad dostępem do baz danych (konta aplikacyjne i użytkowników).