Polityka bezpieczeństwa danych

Numer wersji	Data uchwały Zarządu
1	15 marca 2023

Spis Treści

Rozdział I.
Postanowienia ogólne

§ 1.
Definicje

Użyte w Polityce terminy mają następujące znaczenie:

1) **Administrator** – spółka pod firmą iMercado sp. z o.o.;
2) **Administrator Sieci** – osoba odpowiedzialna za nadzór i prawidłowe funkcjonowanie infrastruktury sieciowej (systemu teleinformatycznego), z której korzysta Administrator;
3) **Dane** – informacje w posiadaniu Administratora, w tym Dane Osobowe;
4) **Dane Osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; 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;

5) **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;
6) **Podmiot Danych** – zidentyfikowana lub możliwa do zidentyfikowania osoba fizyczna;
7) **Podmiot Przetwarzający** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza Dane Osobowe w imieniu Administratora;
8) **Polityka** – niniejsza polityka;
9) **Pracownik** – członek Zarządu lub Rady Nadzorczej Administratora, osoba zatrudniona przez Administratora na podstawie umowy o pracę, a także każda osoba zatrudniona na podstawie umowy zlecenia lub umowy o dzieło lub pozostająca w innym stosunku prawnym o podobnym charakterze z Administratorem;
10) **Prezes Urzędu** – Prezes Urzędu Ochrony Danych Osobowych
11) **Rejestr** – rejestr czynności przetwarzania Danych Osobowych, o którym mowa w art. 30 ust. 1 RODO;
12) **Rejestr Kategorii** – rejestr kategorii czynności przetwarzania, o którym mowa w art. 30 ust. 2 RODO;
13) **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);
14) **Rozporządzenie w sprawie postępowania podmiotów** – rozporządzenie Ministra Finansów z dnia 23 marca 2017 r. w sprawie postępowania podmiotów prowadzących działalność w zakresie pośrednictwa w zbywaniu i odkupywaniu jednostek uczestnictwa oraz tytułów uczestnictwa, a także doradztwa inwestycyjnego w odniesieniu do takich instrumentów;
15) **Strona Trzecia** – osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż Podmiot Danych, Administrator, Podmiot Przetwarzający czy osoby, które – z upoważnienia Administratora lub Podmiotu Przetwarzającego – mogą przetwarzać Dane Osobowe;
16) **System** – system informatyczny (system komputerowy) lub baza danych, wykorzystywane przez Administratora przy przetwarzaniu Danych;
17) **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.

§ 2.
Zakres przedmiotowy regulacji

1. Polityka określa:
   1) źródła standardów i praktyk w zakresie przetwarzania Danych;
   2) osoby wykonujące zadania Administratora;
   3) obszar, w którym przetwarza się Dane;
   4) formy i zasady przetwarzania, przechowywania i dostępu do Danych;
   5) środki organizacyjne i techniczne w celu zapewnienia bezpieczeństwa i integralności Danych;
   6) zasady nadawania uprawnień do przetwarzania Danych;
   7) minimalne standardy w zakresie przetwarzania Danych Osobowych;
   8) zasady tworzenia kopii zapasowych Danych;

9) sposób, miejsce i okres przechowywania Danych;
10) osoby nadzorujące przestrzeganie Polityki przez Pracowników;
11) możliwe konsekwencje naruszenia Polityki przez Pracowników;
12) osoby odpowiedzialne za aktualizację Polityki.

2. Postanowienia Polityki stosuje się do wszystkich Pracowników Administratora, zgodnie z definicją powyżej.
3. Polityka jest procedurą, o której mowa w § 17 ust. 3 Rozporządzenia w sprawie postępowania podmiotów.
4. W zakresie przetwarzania Danych Osobowych Polityka ma pierwszeństwo przed innymi regulacjami wewnętrznymi przyjętymi przez Administratora, niedotyczącymi bezpośrednio przetwarzania Danych Osobowych.

Rozdział II.
Postanowienia szczególne

§ 3.
Podejście do realizacji obowiązków, osoby wykonujące zadania Administratora

1. Podejście do realizacji obowiązków Administratora w przedmiotowym zakresie opiera się na: wymaganiach RODO i innych przepisów powszechnie obowiązujących, rekomendacjach, opiniach i wytycznych właściwych organów nadzorczych, w tym Prezesa Urzędu Ochrony Danych Osobowych, i doradczych, w tym Grupy Roboczej Art. 29 i Europejskiej Rady Ochrony Danych.
2. Z zastrzeżeniem postanowień szczególnych, zadania Administratora przewidziane w Polityce wykonuje, w uzgodnieniu z Zarządem Administratora, Pracownik Administratora wyznaczony przez Zarząd. Pod nieobecność tego Pracownika lub w razie jego niewyznaczenia zadania te wykonuje samodzielnie Zarząd Administratora.
3. Zarząd ma głos decydujący w każdej sprawie. W razie powstania rozbieżności zdań co do konkretnego stanu faktycznego Zarząd przejmuje wykonywanie zadań Administratora w związku z tym konkretnym stanem faktycznym, a Pracownik, o którym mowa w ust. 2, pozostaje zobowiązany udzielać wszelkich porad i wskazówek wymaganych przez Zarząd.

§ 4.
Obszar, w którym przetwarzane są Dane

1. Dane przetwarzane są w siedzibie Administratora, w budynku siedziby mieszczącym się w Warszawie (adres ujawniony w rejestrze przedsiębiorców Krajowego Rejestru Sądowego) oraz w pomieszczeniach zajmowanych przez Podmioty Przetwarzające.

§ 5.
Formy przetwarzania

Dane przetwarzane są:

1) w formie elektronicznej, w Systemie przez pracownika upoważnionego do przetwarzania Danych;
2) w formie papierowej, w zabezpieczonych przed nieuprawnionym dostępem szafach (umowy, zlecenia i dyspozycje Podmiotów Danych, umowy z osobami fizycznymi świadczącymi usługi pośrednictwa w zbywaniu tytułów uczestnictwa, umowy o świadczenie dodatkowe, inne dokumenty).

§ 6.
Sposób przepływu Danych pomiędzy poszczególnymi systemami

W strukturze Administratora nie występuje przepływ Danych pomiędzy poszczególnymi Systemami.

§ 7.
Przechowywanie i dostęp do Danych

1. Dane przechowywane są przez Administratora w formie elektronicznej. Dostęp do Danych posiadają Pracownicy zgodnie z zakresami obowiązków. Dostęp do Danych Osobowych przechowywanych w formie elektronicznej mają wyłącznie osoby upoważnione przez Administratora.
2. Dane mogą być przechowywane także w formie papierowej, w zabezpieczonych przed nieuprawnionym dostępem szafach znajdujących się w siedzibie Administratora. Dostęp do Danych Osobowych przechowywanych w formie papierowej mają wyłącznie osoby upoważnione przez Administratora.

§ 8.
Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności i integralności Danych

1. Obszar, w którym przetwarzane są Dane, w tym infrastrukturę sieciową oraz dokumentację związaną z przetwarzaniem Danych, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w osób upoważnionych do przetwarzania Danych. Przebywanie osób nieuprawnionych w obszarze, w którym przetwarzane są Dane, jest dopuszczalne za zgodą Administratora lub w obecności osoby upoważnionej do przetwarzania Danych.
2. Pomieszczenia, w których przetwarza się Dane, mają zapewnioną ochronę przeciwpożarową.
3. Na tych samych zasadach, co w ust. 1 i 2, zabezpieczone są Dane powierzone Podmiotom Przetwarzającym, co reguluje każdorazowo umowa powierzenia przetwarzania.
4. System chroni się przed zagrożeniami pochodzącymi z sieci publicznej, m.in. poprzez zainstalowanie go w sieci wewnętrznej, stosowanie programu antywirusowego oraz wdrożenie fizycznych zabezpieczeń chroniących przed nieuprawnionym dostępem (sprzętowy firewall). Administrator Sieci monitoruje wdrożone zabezpieczenia Systemu, w tym automatycznie przez całą dobę. Niezwłocznie przeprowadza się uaktualnienia (w razie ich udostępnienia) oraz niezbędne naprawy (w razie ich potrzeby).
5. System zabezpiecza się w szczególności przed:
   1) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
   2) utratą Danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej;
   3) utratą Danych spowodowaną awarią sprzętu (uszkodzeniem sprzętu, na którym działa System).
6. W Systemie stosuje się mechanizmy kontroli dostępu do Danych. Dostęp do każdego z komputerów i Systemu zabezpieczony jest hasłem indywidualnym dla każdego użytkownika. Dodatkowo w komputerach włączone są wygaszacze ekranu zabezpieczone hasłem.
7. Jeżeli dostęp do Danych przetwarzanych w Systemie posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:
   1) w Systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator;
   2) dostęp do Danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.
8. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania Danych, nie może być przydzielony innej osobie.
9. W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne. Hasła nie mogą się powtarzać, jak również nie mogą powtarzać loginu. Niedopuszczalnym jest, aby użytkownicy ujawniali swoje hasła innym osobom.
10. Użytkownik loguje się do Systemu za pomocą swojego loginu i hasła. Po ukończeniu bądź w przypadku przerwy w pracy użytkownik wylogowuje się.

11. W przypadku awarii, zagubienia hasła lub innych nieprzewidzianych sytuacji zagrażających bezpieczeństwu Danych każdy z użytkowników obowiązany jest niezwłocznie powiadomić o tym fakcie Administratora Sieci lub Zarząd Administratora.
12. Osoba użytkująca komputer przenośny zawierający Dane zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, o którym mowa w § 4 ust. 1.
13. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające Dane przeznaczone do:
    1) likwidacji - pozbawia się wcześniej zapisu tych Danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
    2) przekazania podmiotowi nieuprawnionemu do przetwarzania Danych - pozbawia się wcześniej zapisu tych Danych, w sposób uniemożliwiający ich odzyskanie;
    3) naprawy - pozbawia się wcześniej zapisu tych Danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod osobistym nadzorem osoby upoważnionej przez Administratora.
14. W celu usunięcia Danych zawartych w dokumentacji papierowej stosuje się skuteczne metody niszczenia dokumentów, uniemożliwiające ich odtworzenie.

§ 9.
Procedury nadawania uprawnień do przetwarzania Danych Osobowych i rejestrowania tych uprawnień w Systemie oraz wskazanie osoby odpowiedzialnej za te czynności

1. Przetwarzanie Danych Osobowych przez Pracownika nie jest możliwe bez wcześniejszego upoważnienia. Upoważnienie do przetwarzania Danych Osobowych nadawane jest pisemnie przez Zarząd Administratora.
2. Każdy z użytkowników przed uzyskaniem upoważnienia do przetwarzania Danych Osobowych zostaje zobowiązany do zachowania poufności Danych Osobowych objętych Systemem i sposobami ich zabezpieczenia oraz zapoznaje się z wszystkimi regulacjami wewnętrznymi przyjętymi przez Administratora, dotyczącymi przetwarzania Danych Osobowych.
3. Dostęp (login i hasło) do Systemu dla użytkowników upoważnionych do przetwarzania Danych Osobowych nadawany jest przez Administratora Sieci, na polecenie Zarządu Administratora. Administratorowi Sieci przysługuje prawo do zablokowania konta użytkownika w każdym czasie.
4. Administrator prowadzi ewidencję osób upoważnionych do przetwarzania Danych Osobowych, która powinna zawierać:
    1) imię i nazwisko osoby upoważnionej;
    2) datę nadania i ustania oraz zakres upoważnienia do przetwarzania Danych Osobowych;
    3) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

§ 10.
Procedury tworzenia kopii zapasowych Danych Osobowych oraz programów i narzędzi programowych służących do ich przetwarzania

1. Dane Osobowe przetwarzane w Systemie oraz programy i narzędzia programowe służące do ich przetwarzania zabezpiecza się przed utratą przez wykonywanie kopii zapasowych.
2. Kopie zapasowe:
    1) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;
    2) usuwa się niezwłocznie po ustaniu ich użyteczności.

§ 11.
Sposób, miejsce i okres przechowywania

Dla elektronicznych nośników informacji zawierających Dane:

1) Elektronicznymi nośnikami informacji danych są dyski w serwerach.
2) Dostęp do serwerowni jest chroniony przed dostępem osób nieupoważnionych.
3) Okres przechowywania danych jest wskazany w odpowiednich przepisach prawa, a dla Danych Osobowych – w Procedurze retencji i usuwania Danych Osobowych oraz Rejestrze.

Dla kopii zapasowych Danych oraz programów i narzędzi programowych służących do ich przetwarzania:

1) Kopie zapasowe przechowywane są na odrębnym serwerze zewnętrznym, poza budynkiem siedziby Administratora, udostępnionym Administratorowi w celu przechowywania Danych na podstawie odrębnych regulacji i zapewniającym bezpieczeństwo i ochronę Danych na poziomie wymaganym niniejszą Polityką. Dostęp do serwerowni zabezpieczony jest zamkiem.
2) Okres przechowywania w przypadku backupu standardowego, wykonywanego na koniec każdego dnia roboczego, wynosi co najmniej 7 dni, natomiast dla backupu tygodniowego, wykonywanego w każdy piątek, wynosi co najmniej 4 tygodnie.

Rozdział III.
Minimalne standardy w zakresie przetwarzania Danych Osobowych

§ 12.
Środki organizacyjne i techniczne

1. Poniższe postanowienia wyznaczają standard minimalny i nie uchybiają innym postanowieniom Polityki, wyznaczającym wyższy standard bezpieczeństwa.
2. Wymagania w zakresie bezpieczeństwa Danych Osobowych:
   1) zastosowanie, w przypadku uznania za właściwą metodę ochrony, mechanizmów szyfrowania Danych Osobowych lub innych zabezpieczeń, w tym pseudonimizacji, przy czym:
      a) za pseudonimizację uznaje się usunięcie z podstawowej bazy Danych Osobowych informacji mogących zidentyfikować Podmioty Danych; informacje mogące zidentyfikować Podmioty Danych przechowywane są w odrębnej bazie Danych Osobowych o ograniczonym dostępie, niemającej bezpośredniego połączenia z główną bazą Danych Osobowych, która została poddana pseudonimizacji;
      b) za szyfrowanie uznaje się zabezpieczenie przesyłanych Danych Osobowych, baz Danych Osobowych oraz ich kopii zapasowych przed odczytem przez osoby nieuprawnione poprzez zastosowanie algorytmu szyfrującego; odczyt rekordów z zaszyfrowanej bazy Danych Osobowych 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 poprzez:
      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;

i) stosowanie odpowiednio wyższych poziomów zabezpieczeń w przypadku przetwarzania szczególnych kategorii Danych Osobowych, o których mowa w art. 9 ust. 1 RODO, oraz Danych Osobowych dotyczących wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa, o czym mowa w art. 10 RODO, w szczególności poprzez dodatkowe zabezpieczenie hasłem folderów, w których przechowywane są pliki zawierające takie Dane Osobowe, oraz przekazywanie takich plików Podmiotom Przetwarzającym i innym Odbiorcom po uprzednim zabezpieczeniu hasłem, przy czym hasło musi być przekazywane odrębnie i przy zapewnieniu, że otrzyma je osoba uprawniona;

3) zapewnienie dostępności i odporności poprzez:

a) systemy zapewniające dostępność zgodnie z zakresem świadczonych usług;

b) systemy i rozwiązania do wykonywania kopii zapasowych;

c) systemy podtrzymania napięcia (UPS);

d) kontrolę ruchu w sieci wewnętrznej;

e) ograniczanie pojedynczych punktów awarii lub minimalizowanie ryzyka związanego z wykonywaniem awarii;

f) oprogramowanie antywirusowe i kontrolę dostępu do sieci Internet (np. proxy, antyspam);

g) sformalizowane zasady zgłaszania incydentów związanych z bezpieczeństwem systemów;

4) zapewnienie integralności i rozliczalności poprzez:

a) logowanie działalności użytkowników, w szczególności w systemach krytycznych (repozytorium z logami);

b) logowanie wykonanych zmian na Danych Osobowych przez użytkowników, w szczególności w systemach krytycznych;

c) kontrolę jakości danych (w tym m.in. zastosowanie mechanizmów walidacyjnych, weryfikacji poprawności danych – np. maker-checker).

§ 13.
Wymagania funkcjonalne dla Systemów przetwarzających Dane Osobowe

1. Poniższe postanowienia wyznaczają standard minimalny i nie uchybiają innym postanowieniom Polityki, wyznaczającym wyższy standard bezpieczeństwa.
2. Wymagania w zakresie zbierania Danych Osobowych:

1) zakres Danych Osobowych zbieranych i utrzymywanych w Systemie powinien być ograniczony tylko do tych Danych Osobowych, 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, powinien on spełniać poniższe warunki:

a) System powinien umożliwiać równie łatwe udzielenie jak i odwołanie Zgody, które powinno skutkować zaprzestaniem przetwarzania Danych Osobowych 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 lub cofnięcia Zgody powinien być odnotowany w Systemie w sposób zapewniający rozliczalność, w tym poprzez odnotowanie takich danych, jak np. dane personalne osoby wyrażającej Zgodę, data i treść Zgody; jeżeli do przetwarzania Danych Osobowych wykorzystywanych jest kilka Systemów, wystarczające jest odnotowanie Zgody przynajmniej w jednym Systemie.

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

3. Wymagania w zakresie zakończenia lub ograniczenia przetwarzania:

1) System powinien umożliwiać zakończenie przetwarzania Danych Osobowych po upływie oznaczonego okresu; w zależności od dostępnej funkcjonalności Systemu zakończenie przetwarzania może być zrealizowane poprzez usunięcie lub anonimizację Danych Osobowych;

2) System, w zależności od dostępnej funkcjonalności, powinien umożliwiać realizację praw Podmiotów Danych zgodnie z przyjętą przez Administratora procedurą postępowania w celu realizacji tych praw.

3) żadna z powyższych operacji nie może zakłócać integralności Danych Osobowych w Systemach.

4. Wymagania w zakresie jakości Danych Osobowych:

1) System powinien być wyposażony w mechanizmy pozwalające na uaktualniane lub sprostowanie Danych Osobowych (np. w przypadku zmiany Danych Osobowych);

2) System powinien być wyposażony w mechanizmy walidujące lub weryfikujące poprawność wprowadzanych Danych Osobowych (np. algorytmy sprawdzające sumę kontrolną numeru PESEL).

5. Wymagania w zakresie domyślnej ochrony Danych Osobowych („privacy by default"), z zastrzeżeniem postanowień przyjętej przez Administratora polityki przetwarzania Danych Osobowych:

1) Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzane były wyłącznie te Dane Osobowe, które są niezbędne dla osiągniecia celów przetwarzania;

2) obowiązek, o którym mowa w pkt 1, 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) domyślne ustawienia programu (Systemu), w przypadku Systemów 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;

4) ochrona prywatności powinna być realizowana jako domyślne ustawienie każdego programu (Systemu), a zmiana takiego ustawienia powinna być realizowana na wyraźne żądanie Podmiotu Danych jako użytkownika programu.

Rozdział IV.
Postanowienia końcowe

§ 14.
Nadzór nad przestrzeganiem Polityki

1. Nadzór nad przestrzeganiem przez Pracowników Polityki jest sprawowany przez Zarząd.

§ 15.
Postanowienia końcowe

1. Naruszenie Polityki przez osobę zatrudnioną na podstawie umowy o pracę, regulowanej przez przepisy Kodeksu pracy, stanowi rażące naruszenie fundamentalnych obowiązków pracowniczych na podstawie art. 52 § 1 pkt 1 Kodeksu pracy i może prowadzić do nałożenia sankcji przewidzianych w Kodeksie pracy.
2. Za aktualizację Polityki odpowiada Zarząd.

Polityka cookies serwisu www.imercado.pl

Numer wersji	Data uchwały Zarządu
1	15 marca 2023

Serwis www.imercado.pl nie zbiera w sposób automatyczny żadnych informacji, z wyjątkiem informacji zawartych w plikach cookies.

1. Pliki cookies (tzw. „ciasteczka") stanowią dane informatyczne, w szczególności pliki tekstowe, które przechowywane są w urządzeniu końcowym Użytkownika Serwisu i przeznaczone są do korzystania ze stron internetowego Serwisu. Cookies zazwyczaj zawierają nazwę strony internetowej, z której pochodzą, czas przechowywania ich na urządzeniu końcowym oraz unikalny numer.

2. Podmiotem zamieszczającym na urządzeniu końcowym Użytkownika Serwisu pliki cookies oraz uzyskującym do nich dostęp jest operator Serwisu: iMercado sp. z o.o., z siedzibą pod adresem: ul. Jasna 19, 00-058 Warszawa

3. Pliki cookies wykorzystywane są w celu:

a. dostosowania zawartości stron internetowych oraz optymalizacji korzystania ze stron internetowych; w szczególności pliki te pozwalają rozpoznać urządzenie Użytkownika Serwisu i odpowiednio wyświetlić stronę internetową, dostosowaną do jego indywidualnych potrzeb;

5. W ramach Serwisu stosowane są pliki cookies: „sesyjne" (session cookies) . Cookies „sesyjne" są plikami tymczasowymi, które przechowywane są w urządzeniu końcowym Użytkownika do czasu wylogowania, opuszczenia strony internetowej lub wyłączenia oprogramowania (przeglądarki internetowej).

6. W ramach Serwisu stosowane są następujące rodzaje plików cookies:

Nazwa Cookie	Rodzaj i cel zapisania
CMS	sesyjny – Przechowuje identyfikator sesji

7. W wielu przypadkach oprogramowanie służące do przeglądania stron internetowych (przeglądarka internetowa) domyślnie dopuszcza przechowywanie plików cookies w urządzeniu końcowym Użytkownika. Użytkownicy Serwisu mogą dokonać w każdym czasie zmiany ustawień dotyczących plików cookies. Ustawienia te mogą zostać zmienione w szczególności w taki sposób, aby blokować automatyczną obsługę plików cookies w ustawieniach przeglądarki internetowej bądź informować o ich każdorazowym zamieszczeniu w urządzeniu Użytkownika Serwisu. Szczegółowe informacje o możliwości i sposobach obsługi plików cookies dostępne są w ustawieniach oprogramowania (przeglądarki internetowej).

8. Operator Serwisu informuje, że ograniczenia stosowania plików cookies mogą wpłynąć na niektóre funkcjonalności dostępne na stronach internetowych Serwisu.

9. Szczegółowe informacje na temat plików cookies są dostępne pod adresem www.wszystkoociasteczkach.pl lub w sekcji „Pomoc" w menu przeglądarki internetowej.

Polityka przetwarzania danych osobowych

Numer wersji	Data uchwały Zarządu
1	15 marca 2023

Spis Treści

Rozdział I.
Postanowienia ogólne

§ 1.
Definicje

Użyte w Polityce terminy mają następujące znaczenie:

1) **Administrator** – spółka pod firmą iMercado sp. z o.o.;
2) **Dane Osobowe, Dane** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; 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;
3) **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;
4) **Podmiot Danych** – zidentyfikowana lub możliwa do zidentyfikowania osoba fizyczna;
5) **Podmiot Przetwarzający** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza Dane Osobowe w imieniu Administratora;
6) **Polityka** – niniejsza polityka;
7) **Pracownik** – członek Zarządu lub Rady Nadzorczej Administratora, osoba zatrudniona przez Administratora na podstawie umowy o pracę, a także każda osoba zatrudniona na podstawie umowy zlecenia lub umowy o dzieło lub pozostająca w innym stosunku prawnym o podobnym charakterze z Administratorem;

8) **Rejestr** – rejestr czynności przetwarzania Danych Osobowych, o którym mowa w art. 30 ust. 1 RODO;

9) **Rejestr Kategorii** – rejestr kategorii czynności przetwarzania, o którym mowa w art. 30 ust. 2 RODO;

10) **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);

11) **Rozporządzenie w sprawie postępowania podmiotów** – rozporządzenie Ministra Finansów z dnia 23 marca 2017 r. w sprawie postępowania podmiotów prowadzących działalność w zakresie pośrednictwa w zbywaniu i odkupywaniu jednostek uczestnictwa oraz tytułów uczestnictwa, a także doradztwa inwestycyjnego w odniesieniu do takich instrumentów;

12) **Strona Trzecia** – osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż Podmiot Danych, Administrator, Podmiot Przetwarzający czy osoby, które – z upoważnienia Administratora lub Podmiotu Przetwarzającego – mogą przetwarzać Dane Osobowe;

13) **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.

§ 2.
Zakres przedmiotowy regulacji

1. Polityka określa:
   1) źródła standardów i praktyk w zakresie przetwarzania Danych;
   2) osoby wykonujące zadania Administratora;
   3) zasady przetwarzania Danych;
   4) możliwe podstawy przetwarzania Danych;
   5) zasady przetwarzania na podstawie Zgody;
   6) zasady przetwarzania w celu wykonania umowy z Podmiotem Danych;
   7) zasady przetwarzania w celu wypełnienia obowiązku prawnego;
   8) zasady przetwarzania w celu wynikającym z prawnie uzasadnionych interesów Administratora;
   9) zasady uwzględnienia ochrony Danych w fazie projektowania oraz domyślnej ochrony Danych;
   10) osoby nadzorujące przestrzeganie Polityki przez Pracowników;
   11) możliwe konsekwencje naruszenia Polityki przez Pracowników;
   12) osoby odpowiedzialne za aktualizację Polityki.
2. Postanowienia Polityki stosuje się do wszystkich Pracowników Administratora, zgodnie z definicją powyżej.
3. Polityka jest procedurą, o której mowa w § 17 ust. 3 Rozporządzenia w sprawie postępowania podmiotów.
4. W zakresie przetwarzania Danych Osobowych Polityka ma pierwszeństwo przed innymi regulacjami wewnętrznymi przyjętymi przez Administratora, niedotyczącymi bezpośrednio przetwarzania Danych Osobowych.

Rozdział II.
Postanowienia szczególne

§ 3.
Podejście do realizacji obowiązków, osoby wykonujące zadania Administratora

1. Podejście do realizacji obowiązków Administratora w przedmiotowym zakresie opiera się na: wymaganiach RODO i innych przepisów powszechnie obowiązujących, rekomendacjach, opiniach i wytycznych właściwych organów nadzorczych, w tym Prezesa Urzędu Ochrony Danych Osobowych, i doradczych, w tym Grupy Roboczej Art. 29 i Europejskiej Rady Ochrony Danych.
2. Z zastrzeżeniem postanowień szczególnych, zadania Administratora przewidziane w Polityce wykonuje, w uzgodnieniu z Zarządem Administratora, Pracownik Administratora wyznaczony przez Zarząd. Pod nieobecność tego Pracownika lub w razie jego niewyznaczenia zadania te wykonuje samodzielnie Zarząd Administratora.
3. Zarząd ma głos decydujący w każdej sprawie. W razie powstania rozbieżności zdań co do konkretnego stanu faktycznego Zarząd przejmuje wykonywanie zadań Administratora w związku z tym konkretnym stanem faktycznym, a Pracownik, o którym mowa w ust. 2, pozostaje zobowiązany udzielać wszelkich porad i wskazówek wymaganych przez Zarząd.

§ 4.
Zasady przetwarzania Danych

Administrator przetwarza Dane Osobowe Podmiotów Danych:

1. W sposób zgodny z prawem, rzetelny – w szczególności w oparciu o przepisy powszechnie obowiązujące, regulujące funkcjonowanie Administratora, wskazane w § 8 poniżej (przetwarzanie niezbędne prawnie).
2. W konkretnych, wyraźnych i prawnie uzasadnionych celach – w szczególności w oparciu o zasadę celowości, tj.:
    a) w celu wykonania umowy lub podjęcia działań, na żądanie Podmiotu Danych, przed zawarciem tej umowy,
    b) w celu wypełnienia obowiązku prawnego ciążącego na Administratorze,
    c) w celu wynikającym z prawnie uzasadnionych interesów realizowanych przez Administratora lub przez Stronę Trzecią, za które uznaje się w szczególności:
        - marketing bezpośredni usług i produktów oferowanych przez Administratora;
        - prowadzenie marketingu bezpośredniego usług i produktów innych podmiotów (marketing cudzych produktów i usług);
        - dochodzenie i obrona przed roszczeniami;
        - prowadzenie statystyk;
        - ochronę przed próbami oszustwa;
        - bezpieczeństwo świadczonych usług, w tym bezpieczeństwo teleinformatyczne oraz wyjaśnianie okoliczności niedozwolonego korzystania z usług;
        - przesyłanie Danych w ramach grupy kapitałowej;
        - przesyłanie Danych w ramach grupy przedsiębiorstw do wewnętrznych celów administracyjnych;
        - 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.

§ 5.
Podstawy przetwarzania

Administrator przetwarza 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.

§ 6.
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 mowa w art. 22 ust. 1 i 4 RODO, przekazywanie Danych Osobowych do państwa trzeciego na podstawie Zgody lub przetwarzanie szczególnych kategorii Danych Osobowych, o których mowa w art. 9 ust. 1 RODO, 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.
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 za przestrzeganie przez Administratora 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-upów lub zrzutów z ekranu), odznaczenie odpowiednich symboli (ticków) w bazach danych, posiadanie stosownych polityk i procedur wewnętrznych oraz notatek z przebiegu spotkań.

§ 7.
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.

§ 8.
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 Administratora obejmują w szczególności:
   1) ustawę z dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi;
   2) ustawę z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych;
   3) ustawę z dnia 9 marca 2017 r. o wymianie informacji podatkowych z innymi państwami;
   4) 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;
   5) ustawę z dnia 5 sierpnia 2015 r. o rozpatrywaniu reklamacji przez podmioty rynku finansowego i o Rzeczniku Finansowym;
   6) ustawę z dnia 23 kwietnia 1964 r. Kodeks cywilny;
   7) ustawę z dnia 20 kwietnia 2004 r. o pracowniczych programach emerytalnych;
   8) ustawę z dnia 20 kwietnia 2004 r. o indywidualnych kontach emerytalnych oraz indywidualnych kontach zabezpieczenia emerytalnego;
   9) ustawę z dnia 4 lutego 1994 r. o prawach autorskich i prawach pokrewnych;
   10) ustawę z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną.
3. W przypadku gdy Administrator 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.

§ 9.
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 § 4 ust. 2 lit. c Polityki.

§ 10.
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. 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.

Rozdział III.
Postanowienia końcowe

§ 11.
Nadzór nad przestrzeganiem Polityki

1. Nadzór nad przestrzeganiem przez Pracowników Polityki jest sprawowany przez Zarząd.

§ 12.
Postanowienia Końcowe

1. Naruszenie Polityki przez osobę zatrudnioną na podstawie umowy o pracę, regulowanej przez przepisy Kodeksu pracy, stanowi rażące naruszenie fundamentalnych obowiązków pracowniczych na podstawie art. 52 § 1 pkt 1 Kodeksu pracy i może prowadzić do nałożenia sankcji przewidzianych w Kodeksie pracy.
2. Za aktualizację Polityki odpowiada Zarząd.

Procedura oceny skutków dla ochrony danych osobowych

Numer wersji	Data uchwały Zarządu
1	15 marca 2023

Spis Treści

Rozdział I.
Postanowienia ogólne

§ 1.
Definicje

Użyte w Procedurze terminy mają następujące znaczenie:

1) **Administrator** – spółka pod firmą iMercado sp. z o.o.;
2) **Dane Osobowe, Dane** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; 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;
3) **Ocena** – ocena skutków planowanych operacji przetwarzania dla ochrony Danych Osobowych, o której mowa w art. 35 ust. 1 RODO;
4) **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;
5) **Podmiot Danych** – zidentyfikowana lub możliwa do zidentyfikowania osoba fizyczna;
6) **Podmiot Przetwarzający –** osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza Dane Osobowe w imieniu Administratora;
7) **Procedura –** niniejsza procedura;
8) **Pracownik –** członek Zarządu lub Rady Nadzorczej Administratora, osoba zatrudniona przez Administratora na podstawie umowy o pracę, a także każda osoba zatrudniona na podstawie umowy zlecenia lub umowy o dzieło lub pozostająca w innym stosunku prawnym o podobnym charakterze z Administratorem;
9) **Rejestr –** rejestr czynności przetwarzania Danych Osobowych, o którym mowa w art. 30 ust. 1 RODO;

10) **Rejestr Kategorii –** rejestr kategorii czynności przetwarzania, o którym mowa w art. 30 ust. 2 RODO;

11) **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);

12) **Rozporządzenie w sprawie postępowania podmiotów** – rozporządzenie Ministra Finansów z dnia 23 marca 2017 r. w sprawie postępowania podmiotów prowadzących działalność w zakresie pośrednictwa w zbywaniu i odkupywaniu jednostek uczestnictwa oraz tytułów uczestnictwa, a także doradztwa inwestycyjnego w odniesieniu do takich instrumentów;

13) **Strona Trzecia** – osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż Podmiot Danych, Administrator, Podmiot Przetwarzający czy osoby, które – z upoważnienia Administratora lub Podmiotu Przetwarzającego – mogą przetwarzać Dane Osobowe.

§ 2.
Zakres przedmiotowy regulacji

1. Procedura określa:
   1) źródła standardów i praktyk w zakresie przetwarzania Danych;
   2) osoby wykonujące zadania Administratora;
   3) przypadki, gdy dokonanie Oceny jest konieczne, nie jest konieczne lub wymaga rozważenia;
   4) zasady dokonywania Oceny;
   5) zasady konsultacji z organem nadzorczym;
   6) osoby nadzorujące przestrzeganie Procedury przez Pracowników;
   7) możliwe konsekwencje naruszenia Procedury przez Pracowników;
   8) osoby odpowiedzialne za aktualizację Procedury.
2. Postanowienia Procedury stosuje się do wszystkich Pracowników Administratora, zgodnie z definicją powyżej.
3. Procedura jest procedurą, o której mowa w § 17 ust. 3 Rozporządzenia w sprawie postępowania podmiotów.
4. W zakresie przetwarzania Danych Osobowych Procedura ma pierwszeństwo przed innymi regulacjami wewnętrznymi przyjętymi przez Administratora, niedotyczącymi bezpośrednio przetwarzania Danych Osobowych.

Rozdział II.
Postanowienia szczególne

§ 3.
Podejście do realizacji obowiązków, osoby wykonujące zadania Administratora

1. Podejście do realizacji obowiązków Administratora w przedmiotowym zakresie opiera się na: wymaganiach RODO i innych przepisów powszechnie obowiązujących, rekomendacjach, opiniach i wytycznych właściwych organów nadzorczych, w tym Prezesa Urzędu Ochrony Danych Osobowych, i doradczych, w tym Grupy Roboczej Art. 29 i Europejskiej Rady Ochrony Danych.
2. Z zastrzeżeniem postanowień szczególnych, zadania Administratora przewidziane w Procedurze wykonuje, w uzgodnieniu z Zarządem Administratora, Pracownik Administratora wyznaczony przez Zarząd. Pod nieobecność tego Pracownika lub w razie jego niewyznaczenia zadania te wykonuje samodzielnie Zarząd Administratora.

3. Zarząd ma głos decydujący w każdej sprawie. W razie powstania rozbieżności zdań co do konkretnego stanu faktycznego Zarząd przejmuje wykonywanie zadań Administratora w związku z tym konkretnym stanem faktycznym, a Pracownik, o którym mowa w ust. 2, pozostaje zobowiązany udzielać wszelkich porad i wskazówek wymaganych przez Zarząd.

§ 4.
Dokonywanie Oceny

1. Jeżeli dany rodzaj przetwarzania Danych – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności Podmiotów Danych Osobowych, Administrator przed rozpoczęciem przetwarzania dokonuje Oceny.
2. Administrator jest obowiązany dokonać Oceny w szczególności w przypadku:
   1) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do Podmiotów Danych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec Podmiotu Danych lub w podobny sposób znacząco wpływających na Podmiot Danych; lub
   2) przetwarzania na dużą skalę szczególnych kategorii Danych Osobowych, o których mowa w art. 9 ust. 1 RODO (tzn. Danych Osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania Podmiotu Danych lub danych dotyczących zdrowia, seksualności albo orientacji seksualnej Podmiotu Danych), lub Danych Osobowych dotyczących wyroków skazujących i czynów zabronionych, o czym mowa w art. 10 RODO; lub
   3) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie; lub
   4) gdy dany rodzaj przetwarzania został wskazany w wykazie podanym do publicznej wiadomości przez organ nadzorczy, zgodnie z art. 35 ust. 4 RODO.
3. Z zastrzeżeniem ust. 1 i 2, Administrator jest dodatkowo obowiązany rozważyć dokonanie Oceny w następujących sytuacjach:
   1) przed wykorzystaniem nowych technologii przetwarzania Danych, takich jak np. nowych systemów informatycznych, wprowadzania istotnych modyfikacji do istniejących systemów;
   2) przed wprowadzeniem nowej usługi lub nowego typu produktu;
   3) przed przejęciem Danych od innych Administratorów;

   - pod warunkiem, że przetwarzanie ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności Podmiotów Danych.
4. Administrator może też dokonać Oceny, mimo że dany rodzaj przetwarzania został wskazany w wykazie podanym do publicznej wiadomości przez organ nadzorczy, zgodnie z art. 35 ust. 5 RODO.
5. Administrator nie jest obowiązany dokonać Oceny, jeżeli przetwarzanie na mocy art. 6 ust. 1 lit. c) lub e) RODO ma podstawę prawną w prawie Unii Europejskiej lub w prawie państwa członkowskiego, któremu podlega Administrator, i prawo takie reguluje daną operację przetwarzania lub zestaw operacji, a Oceny dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej, tzn. Oceny dokonano już na etapie prac legislacyjnych – chyba że państwa członkowskie uznają za niezbędne, by przed podjęciem czynności przetwarzania dokonać Oceny.
6. Dla podobnych operacji przetwarzania Danych, wiążących się z podobnym ryzykiem, można przeprowadzić pojedynczą Ocenę.
7. Ocena zawiera co najmniej:

1) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez Administratora;
2) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
3) ocenę ryzyka naruszenia praw lub wolności Podmiotów Danych; oraz
4) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę Danych Osobowych i wykazać przestrzeganie RODO, z uwzględnieniem praw i prawnie uzasadnionych interesów Podmiotów Danych i innych osób, których sprawa dotyczy.

8. Oceniając skutki operacji przetwarzania wykonywanych przez Administratora lub Administratora działającego jako Podmiot Przetwarzający, uwzględnia się przestrzeganie zatwierdzonych kodeksów postępowania, o których mowa w art. 40 RODO, o ile Administrator je stosuje, a także dokumentu „Wytyczne dotyczące skutków dla ochrony danych oraz pomagające ustalić, czy „przetwarzanie może powodować wysokie ryzyko" do celów rozporządzenia 2016/679", przyjętego w dniu 4 kwietnia 2017 r. przez Grupę Roboczą art. 29, WP 248, w brzmieniu aktualnym na dzień dokonania Oceny.
9. W stosownych przypadkach Administrator zasięga opinii Podmiotów Danych lub ich przedstawicieli w sprawie zamierzonego przetwarzania, bez uszczerbku dla ochrony interesów handlowych lub publicznych lub bezpieczeństwa operacji przetwarzania. Oznacza to, że Administrator nie ma obowiązku zasięgania opinii w każdym przypadku, a jedynie wówczas, gdy takie opinie mogą mieć istotne znaczenie dla Oceny, natomiast przy zasięganiu opinii Administrator nie ma obowiązku podawania informacji, które mogłyby powodować zagrożenie jego interesów handlowych (np. ujawnienie tajemnicy przedsiębiorstwa) lub bezpieczeństwa operacji przetwarzania (np. ujawnienie szczegółowych informacji o zabezpieczeniach).
10. W razie potrzeby, przynajmniej gdy zmienia się ryzyko wynikające z operacji przetwarzania, Administrator dokonuje przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z Oceną.
11. Informację o dokonaniu Oceny zamieszcza się odpowiednio w Rejestrze lub Rejestrze Kategorii.

§ 5.
Konsultacje z organem nadzorczym

1. W przypadku w którym Ocena wykaże, 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.
2. Konsultując się z organem nadzorczym zgodnie z ust. 1, Administrator przedstawia mu:
   1) gdy ma to zastosowanie - odpowiednie obowiązki Administratora, współadministratorów oraz Podmiotów Przetwarzających uczestniczących w przetwarzaniu, w szczególności w przypadku przetwarzania w ramach grupy przedsiębiorstw;
   2) cele i sposoby zamierzonego przetwarzania;
   3) środki i zabezpieczenia mające chronić prawa i wolności Podmiotów Danych;
   4) dane kontaktowe Inspektora, o ile został wyznaczony;
   5) Ocenę; oraz
   6) wszelkie inne informacje, których żąda organ nadzorczy.

Rozdział III.
Postanowienia końcowe

§ 6.
Nadzór nad przestrzeganiem Procedury

1. Nadzór nad przestrzeganiem przez Pracowników Procedury jest sprawowany przez Zarząd.

§ 7.
Postanowienia końcowe

1. Naruszenie Procedury przez osobę zatrudnioną na podstawie umowy o pracę, regulowanej przez przepisy Kodeksu pracy, stanowi rażące naruszenie fundamentalnych obowiązków pracowniczych na podstawie art. 52 § 1 pkt 1 Kodeksu pracy i może prowadzić do nałożenia sankcji przewidzianych w Kodeksie pracy.
2. Za aktualizację Procedury odpowiada Zarząd.

Procedura postępowania w celu realizacji praw podmiotów danych osobowych

Numer wersji	Data uchwały Zarządu
1	15 marca 2023

Spis Treści

Rozdział I.
Postanowienia ogólne

§ 1.
Definicje

Użyte w Procedurze terminy mają następujące znaczenie:

1) **Administrator** – spółka pod firmą iMercado sp. z o.o.;
2) **Dane Osobowe, Dane** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; 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;
3) **Ocena** – ocena skutków planowanych operacji przetwarzania dla ochrony Danych Osobowych, o której mowa w art. 35 ust. 1 RODO;
4) **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;

5) **Podmiot Danych** – zidentyfikowana lub możliwa do zidentyfikowania osoba fizyczna;
6) **Podmiot Przetwarzający –** osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza Dane Osobowe w imieniu Administratora;
7) **Procedura –** niniejsza procedura;
8) **Pracownik –** członek Zarządu lub Rady Nadzorczej Administratora, osoba zatrudniona przez Administratora na podstawie umowy o pracę, a także każda osoba zatrudniona na podstawie umowy zlecenia lub umowy o dzieło lub pozostająca w innym stosunku prawnym o podobnym charakterze z Administratorem;
9) **Rejestr –** rejestr czynności przetwarzania Danych Osobowych, o którym mowa w art. 30 ust. 1 RODO;
10) **Rejestr Kategorii –** rejestr kategorii czynności przetwarzania, o którym mowa w art. 30 ust. 2 RODO;
11) **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);
12) **Rozporządzenie w sprawie postępowania podmiotów** – rozporządzenie Ministra Finansów z dnia 23 marca 2017 r. w sprawie postępowania podmiotów prowadzących działalność w zakresie pośrednictwa w zbywaniu i odkupywaniu jednostek uczestnictwa oraz tytułów uczestnictwa, a także doradztwa inwestycyjnego w odniesieniu do takich instrumentów;
13) **Strona Trzecia** – osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż Podmiot Danych, Administrator, Podmiot Przetwarzający czy osoby, które – z upoważnienia Administratora lub Podmiotu Przetwarzającego – mogą przetwarzać Dane Osobowe.

§ 2.
Zakres przedmiotowy regulacji

1. Procedura określa:
   1) źródła standardów i praktyk w zakresie przetwarzania Danych;
   2) osoby wykonujące zadania Administratora;
   3) zasady realizacji przez Administratora wszystkich praw Podmiotów Danych;
   4) zasady realizacji przez Administratora poszczególnych praw Podmiotów Danych;
   5) zasady prowadzenia rejestru żądań zgłoszonych przez Podmioty Danych;
   6) osoby nadzorujące przestrzeganie Procedury przez Pracowników;
   7) możliwe konsekwencje naruszenia Procedury przez Pracowników;
   8) osoby odpowiedzialne za aktualizację Procedury.
2. Postanowienia Procedury stosuje się do wszystkich Pracowników Administratora, zgodnie z definicją powyżej.
3. Procedura jest procedurą, o której mowa w § 17 ust. 3 Rozporządzenia w sprawie postępowania podmiotów.
4. W zakresie przetwarzania Danych Osobowych Procedura ma pierwszeństwo przed innymi regulacjami wewnętrznymi przyjętymi przez Administratora, niedotyczącymi bezpośrednio przetwarzania Danych Osobowych.

Rozdział II.
Postanowienia szczególne

§ 3.
Podejście do realizacji obowiązków, osoby wykonujące zadania Administratora

1. Podejście do realizacji obowiązków Administratora w przedmiotowym zakresie opiera się na: wymaganiach RODO i innych przepisów powszechnie obowiązujących, rekomendacjach, opiniach i wytycznych właściwych organów nadzorczych, w tym Prezesa Urzędu Ochrony Danych Osobowych, i doradczych, w tym Grupy Roboczej Art. 29 i Europejskiej Rady Ochrony Danych.
2. Z zastrzeżeniem postanowień szczególnych, zadania Administratora przewidziane w Procedurze wykonuje, w uzgodnieniu z Zarządem Administratora, Pracownik Administratora wyznaczony przez Zarząd. Pod nieobecność tego Pracownika lub w razie jego niewyznaczenia zadania te wykonuje samodzielnie Zarząd Administratora.
3. Zarząd ma głos decydujący w każdej sprawie. W razie powstania rozbieżności zdań co do konkretnego stanu faktycznego Zarząd przejmuje wykonywanie zadań Administratora w związku z tym konkretnym stanem faktycznym, a Pracownik, o którym mowa w ust. 2, pozostaje zobowiązany udzielać wszelkich porad i wskazówek wymaganych przez Zarząd.

§ 4.
Zasady realizacji wszystkich praw Podmiotów Danych

1. Administrator realizuje prawa Podmiotu Danych, w szczególności w zakresie:
   1) Prawa do informacji (realizacja obowiązku informacyjnego);
   2) Prawa dostępu do Danych;
   3) Prawa do sprostowania Danych;
   4) Prawa do usunięcia Danych („prawo do bycia zapomnianym”);
   5) Prawa do ograniczenia przetwarzania;
   6) Prawa do przenoszenia Danych;
   7) 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 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:
   1) pisemnie;
   2) ustnie;
   3) w sposób elektroniczny;
   4) 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:

1) 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;

2) wskazanie zakresu Danych i czynności, których wniosek dotyczy.

6. Terminy odpowiedzi na żądania lub realizacji praw Podmiotu Danych przez Administratora (chyba że w dalszej części Procedury postanowiono inaczej):

   1) 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;

   2) 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.

7. Realizacja praw Podmiotu Danych, oraz podejmowanie działań na jego żądanie, są wolne od opłat, z zastrzeżeniem ust. 8.

8. 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.

9. Administrator jest uprawniony do pobrania opłaty, o której mowa w ust. 8, w sytuacji gdy żądanie:

   1) 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;

   2) dotyczy informacji dzielonych na kilka lub kilkanaście żądań;

   3) dotyczy wniosku o szczególny nośnik lub format odpowiedzi, jeżeli nie odpowiada on standardowemu formatowi przyjętemu przez Administratora i jednocześnie powszechnie stosowanemu w obrocie;

   4) dotyczy wniosku o udzielenie odpowiedzi w języku innym niż język polski, chyba że w komunikacji z Podmiotem Danych standardowo stosowany jest inny język;

   5) dotyczy wniosku, którego realizacja wymaga zaangażowania zasobów ludzkich lub środków niezbędnych do prawidłowego wykonania wniosku w stopniu zakłócającym normalną działalność Administratora, np. wniosku o bardzo szczegółowe informacje;

   6) ma zostać zrealizowane w szczególnym trybie jak np. odpowiedź przesłana kurierem.

10. W przypadku gdy Administrator będzie uprawniony do naliczenia opłaty za realizację wniosku Podmiotu Danych zgodnie z ust. 8 i 9, poinformuje wcześniej Podmiot Danych o wysokości opłaty oraz numerze konta bankowego i rozpocznie realizację wniosku po otrzymaniu takiej opłaty.

11. Administrator jest uprawniony do odmowy podjęcia działań w związku z żądaniem Podmiotu Danych w sytuacji gdy:

   1) żądanie ma zostać zrealizowane w formacie lub na nośniku, który nie jest obsługiwany przez Administratora lub nie spełnia podstawowych standardów bezpieczeństwa;

   2) wniosek jest niejasny i nieprecyzyjny, a Podmiot Danych składający wniosek, pomimo prośby o uzupełnienie brakujących informacji, nadal jej nie zrealizował;

   3) 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;

   4) Podmiot Danych nie uiścił opłaty, o której mowa w ust. 8 - 10;

5) 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.

12. W przypadku, o którym mowa w ust. 11, Administrator informuje o powodach niepodjęcia działań oraz możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

13. 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.

§ 5.
Prawo do informacji

1. Uprawnieniu do uzyskania informacji o przetwarzaniu Danych Osobowych, istniejącemu po stronie Podmiotu Danych, odpowiada obowiązek informacyjny po stronie Administratora. Obowiązek ten 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 bezpośrednio od Podmiotu Danych zakres informacji przekazywanych Podmiotowi Danych przez Administratora obejmuje co najmniej:

   1) nazwę, adres, dane kontaktowe oraz, gdy ma to zastosowanie – tożsamość i dane kontaktowe swojego przedstawiciela;

   2) gdy ma to zastosowanie - dane kontaktowe inspektora ochrony danych;

   3) cele przetwarzania Danych;

   4) podstawę prawną przetwarzania Danych;

   5) prawnie uzasadnione interesy realizowane przez Administratora, jeżeli przetwarzanie Danych odbywa się na podstawie art. 6 ust. 1 lit. f) RODO;

   6) informację o odbiorcach lub kategoriach odbiorców (jeśli istnieją), którym Dane zostały lub zostaną ujawnione (w szczególności obiorcy w państwach trzecich lub organizacjach międzynarodowych);

   7) jeżeli ma to zastosowanie, informację o zamiarze przekazania Danych Osobowych do państwa trzeciego na zasadach wskazanych w art. 13 ust. 1 lit. f RODO;

   8) okres, przez który Dane Osobowe będą przechowywane, a gdy nie jest to możliwe – kryteria ustalania tego okresu;

   9) 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;

   10) 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;

   11) informację o prawie wniesienia skargi do organu nadzorczego;

   12) 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;

13) 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.

3. W przypadku pozyskiwania Danych Osobowych niebezpośrednio od Podmiotu Danych zakres informacji przekazywanych Podmiotowi Danych przez Administratora obejmuje informacje wskazane w ust. 2 lit. a)-k) i m) oraz dodatkowo:

   1) kategorie odnośnych Danych Osobowych;

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

4. W przypadku zmiany celów przetwarzania Danych Osobowych i, w związku z tym, pozyskiwania dodatkowych Danych Osobowych bezpośrednio od Podmiotu Danych zakres informacji przekazywanych Podmiotowi Danych przez Administratora obejmuje co najmniej:

   1) cele przetwarzania Danych;

   2) okres, przez który Dane Osobowe będą przechowywane, a gdy nie jest to możliwe – kryteriach ustalania tego okresu;

   3) 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;

   4) 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;

   5) informację o prawie wniesienia skargi do organu nadzorczego;

   6) 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;

   7) 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 i, w związku z tym, pozyskiwania dodatkowych Danych Osobowych niebezpośrednio od Podmiotu Danych zakres informacji przekazywanych Podmiotowi Danych przez Administratora obejmuje informacje wskazane w ust. 4 lit. a)-e) i g) oraz dodatkowo:

   1) prawnie uzasadnione interesy realizowane przez Administratora, jeżeli przetwarzanie Danych odbywa się na podstawie art. 6 ust. 1 lit. f) RODO;

   2) 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 niebezpośrednio od Podmiotu Danych informacja jest przekazywana:

   1) w rozsądnym terminie, nie później jednak niż w terminie miesiąca od pozyskania Danych;

   2) najpóźniej przy pierwszej komunikacji z Podmiotem Danych, jeżeli Dane Osobowe mają być stosowane do komunikacji z tą osobą;

3) najpóźniej przy pierwszym ujawnieniu Danych, jeżeli Administrator planuje ujawnić Dane Osobowe innemu odbiorcy.

8. Klauzule informacyjne mogą być przekazywane z zastosowaniem obowiązujących standardów bezpieczeństwa:
   1) pisemnie;
   2) ustnie;
   3) w sposób elektroniczny;
   4) w innej formie – akceptowalnej i umożliwiającej udokumentowanie realizacji przedmiotowego obowiązku.
9. Obowiązki informacyjne w odniesieniu do uczestników funduszy inwestycyjnych i w zakresie danych przetwarzanych w związku z uczestnictwem w funduszach wykonują poszczególne fundusze inwestycyjne jako administratorzy tych danych. Klauzule informacyjne przekazywane są przez fundusze inwestycyjne w dokumentach przeznaczonych dla uczestników lub w systemie informatycznym po potwierdzeniu tożsamości Podmiotu Danych lub poprzez przesłanie informacji drogą elektroniczną, z zastosowaniem standardów bezpieczeństwa. W zakresie jednak, w jakim Administrator przetwarza dane uczestników funduszy inwestycyjnych jako administrator, Administrator samodzielnie i we własnym imieniu wypełnia obowiązki informacyjne.
10. Obowiązek informacyjny w stosunku do Podmiotów Danych nie jest realizowany przez Administratora, jeżeli:
    1) Podmiot Danych dysponuje już tymi informacjami (np. zbieranie dodatkowych Danych Osobowych w tym samym celu);
    2) udzielenie informacji osobie, której Dane zostały zebrane niebezpośrednio od niej, jest niemożliwe (np. brak adresu) lub wymagałoby niewspółmiernie dużego wysiłku albo wymagałoby pozyskiwania informacji dodatkowych z innych źródeł zewnętrznych. Do takich sytuacji zaliczyć należy, przy każdorazowym spełnieniu przesłanek wskazanych w zdaniu poprzedzającym, m.in. przetwarzanie Danych pełnomocników, przedstawicieli ustawowych, członków zarządu i reprezentantów zawartych w odpisach z Krajowego Rejestru Sądowego; przedmiotowe zwolnienie dotyczy też przypadku przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych (z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 89 ust. 1 RODO);
    3) pozyskanie lub ujawnienie Danych osoby, której Dane są zebrane niebezpośrednio od niej, uregulowane jest w przepisach prawa przewidujących ochronę prawnie uzasadnionych interesów Podmiotu Danych;
    4) Dane Osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej, tajemnicy przedsiębiorstwa oraz innych tajemnic ustawowo chronionych;
    5) przepis szczególny wyłącza obowiązek informacyjny na podstawie art. 23 ust. 1 RODO.
11. 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 takich Podmiotów Danych oraz osób, którym udzielenie informacji okaże się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku albo wymagałoby pozyskiwania informacji dodatkowych z innych źródeł zewnętrznych, obowiązek ten może zostać zrealizowany poprzez umieszczenie informacji na własnej stronie internetowej.

§ 6.
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:

1) celów przetwarzania (np. wykonywanie umowy, wypełnienie obowiązków prawnych ciążących na Administratorze, realizacja celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora);
2) kategorii odnośnych Danych Osobowych;
3) odbiorcy lub kategorii odbiorców, którym Dane Osobowe zostały lub mogą zostać ujawnione, w szczególności odbiorców w państwach trzecich lub organizacjach międzynarodowych (np. podmioty świadczące usługi doradcze, audytowe, księgowe, prawne, informatyczne, archiwizacji i niszczenia dokumentów, marketingowe, jak również biegli rewidenci w związku z audytem);
4) 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;
5) informacji o prawie do żądania sprostowania, usunięcia lub ograniczenia przetwarzania Danych Osobowych dotyczącego Podmiotu Danych oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
6) informacji o prawie wniesienia skargi do organu nadzorczego;
7) jeżeli Dane Osobowe nie zostały zebrane od Podmiotu Danych – wszelkich dostępnych informacji o ich źródle;
8) 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 o fakcie zatwierdzenia przez organ nadzorczy kodeksu postępowania.
3. Administrator może udostępnić Podmiotom Danych kanał, za pomocą którego można będzie 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 § 3 ust. 8 i 9 Procedury, na zasadach określonych § 3 ust. 10 Procedury.
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 udostępnienie 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.

§ 7.
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.

§ 8.
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.

§ 9.
Prawo do ograniczenia przetwarzania Danych Osobowych

1. Podmiotowi Danych przysługuje prawo do żądania od Administratora ograniczenia przetwarzania Danych Osobowych 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 którym 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.
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.

§ 10.
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 z postanowieniami 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.

§ 11.
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.
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 1 do Procedury.
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. W przypadku Podmiotów Danych – uczestników funduszy inwestycyjnych katalog Danych Osobowych podlegających przenoszeniu został wskazany w Załączniku nr 1 do Procedury. W innych przypadkach zakres Danych Osobowych jest ustalany przez Administratora w zależności od konkretnego stanu faktycznego. Bez względu na sytuację 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 przeniesienia 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 1 do Procedury;
   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 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 i regulacji wewnętrznych przyjętych przez Administratora.

§ 12.
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.

§ 13.
Przenoszenie Danych poprzez przesłanie innemu Administratorowi

1. W przypadku wniosku o przesłanie Danych do innego administratora, bezpośrednie przesłanie Danych przez Administratora jako „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. Przesłanie Danych do administratora „odbierającego" nie oznacza zawarcia przez Podmiot Danych umowy ani nawiązania jakiegokolwiek stosunku umownego z administratorem „odbierającym".
3. Na wniosek Podmiotu Danych Administrator w miarę możliwości przekaże Dane Osobowe wskazane we wniosku administratorowi „odbierającemu". Jeśli 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 zwolnieniu Administratora jako „przekazującego" z obowiązku zachowania tajemnicy zawodowej w tym zakresie. W braku takiego oświadczenia Administrator przekaże Dane bezpośrednio Podmiotowi Danych lub wstrzyma się z realizacją żądania do czasu otrzymania odpowiedniego oświadczenia.
5. Administrator jako „przekazujący" Dane Osobowe, odpowiadając 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).

§ 14.
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 wykaże istnienie podstaw do ustalenia, dochodzenia lub obrony roszczeń. Do sytuacji, w których Administrator będzie mógł przetwarzać Dane pomimo wniesienia sprzeciwu zaliczyć można w szczególności następujące prawnie uzasadnione interesy realizowane przez Administratora: dochodzenie i obronę przed roszczeniami, prowadzenie statystyk, ochronę przed próbami oszustwa, bezpieczeństwo świadczonych usług, w tym bezpieczeństwo teleinformatyczne oraz wyjaśnianie okoliczności niedozwolonego korzystania z usług.
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 § 9 Procedury.
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.

§ 15.
Rejestr

1. W celu zapewnienia rozliczalności Administrator prowadzi rejestr wszystkich żądań zgłoszonych przez Podmioty Danych.
2. Rejestr jest prowadzony w formie papierowej lub elektronicznej, w taki sposób, aby w każdej chwili mógł być udostępniony organowi nadzorczemu w celu weryfikacji przestrzegania wymogów określonych w RODO.
3. W przypadku otrzymania żądania od Podmiotu Danych Administrator dokumentuje ten fakt, treść otrzymanego żądania oraz sposób jego załatwienia.

Rozdział III.
Postanowienia końcowe

§ 16.
Nadzór nad przestrzeganiem Procedury

1. Nadzór nad przestrzeganiem przez Pracowników Procedury jest sprawowany przez Zarząd.

§ 17.
Postanowienia końcowe

1. Naruszenie Procedury przez osobę zatrudnioną na podstawie umowy o pracę, regulowanej przez przepisy Kodeksu pracy, stanowi rażące naruszenie fundamentalnych obowiązków pracowniczych na podstawie art. 52 § 1 pkt 1 Kodeksu pracy i może prowadzić do nałożenia sankcji przewidzianych w Kodeksie pracy.
2. Za aktualizację Procedury odpowiada Zarząd.

Załącznik nr 1
do Procedury postępowania w celu realizacji praw podmiotów danych osobowych

KATALOG DANYCH UCZESTNIKÓW FUNDUSZY INWESTYCYJNYCH PODLEGAJĄCYCH PRZENOSZENIU

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 ▪ Liczba jednostek uczestnictwa / certyfikatów
STOSOWANY FORMAT	
XLS, CSV, XML, HTML	

Procedura postępowania w przypadku naruszeń ochrony danych osobowych

Numer wersji	Data uchwały Zarządu
1	15 marca 2023

Spis Treści

Rozdział I.
Postanowienia ogólne

§ 1.
Definicje

Użyte w Procedurze terminy mają następujące znaczenie:

1) **Administrator** – spółka pod firmą iMercado sp. z o.o.;
2) **Dane Osobowe, Dane** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; 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;
3) **Incydent** – naruszenie ochrony Danych Osobowych, przez co rozumie się 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;
4) **Ocena** – ocena skutków planowanych operacji przetwarzania dla ochrony Danych Osobowych, o której mowa w art. 35 ust. 1 RODO;
5) **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;
6) **Podmiot Danych** – zidentyfikowana lub możliwa do zidentyfikowania osoba fizyczna;
7) **Podmiot Przetwarzający –** osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza Dane Osobowe w imieniu Administratora;

8) **Procedura –** niniejsza procedura;

9) **Pracownik –** członek Zarządu lub Rady Nadzorczej Administratora, osoba zatrudniona przez Administratora na podstawie umowy o pracę, a także każda osoba zatrudniona na podstawie umowy zlecenia lub umowy o dzieło lub pozostająca w innym stosunku prawnym o podobnym charakterze z Administratorem;

10) **Rejestr –** rejestr czynności przetwarzania Danych Osobowych, o którym mowa w art. 30 ust. 1 RODO;

11) **Rejestr Kategorii –** rejestr kategorii czynności przetwarzania, o którym mowa w art. 30 ust. 2 RODO;

12) **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);

13) **Rozporządzenie w sprawie postępowania podmiotów** – rozporządzenie Ministra Finansów z dnia 23 marca 2017 r. w sprawie postępowania podmiotów prowadzących działalność w zakresie pośrednictwa w zbywaniu i odkupywaniu jednostek uczestnictwa oraz tytułów uczestnictwa, a także doradztwa inwestycyjnego w odniesieniu do takich instrumentów;

14) **Strona Trzecia** – osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż Podmiot Danych, Administrator, Podmiot Przetwarzający czy osoby, które – z upoważnienia Administratora lub Podmiotu Przetwarzającego – mogą przetwarzać Dane Osobowe.

§ 2.
Zakres przedmiotowy regulacji

1. Procedura określa:
   1) źródła standardów i praktyk w zakresie przetwarzania Danych;
   2) osoby wykonujące zadania Administratora;
   3) postępowanie w przypadku podejrzenia naruszenia RODO, innych przepisów o ochronie Danych Osobowych lub regulacji wewnętrznych dotyczących ochrony Danych Osobowych;
   4) postępowanie w przypadku stwierdzenia Incydentu;
   5) osoby nadzorujące przestrzeganie Procedury przez Pracowników;
   6) możliwe konsekwencje naruszenia Procedury przez Pracowników;
   7) osoby odpowiedzialne za aktualizację Procedury.
2. Postanowienia Procedury stosuje się do wszystkich Pracowników Administratora, zgodnie z definicją powyżej.
3. Procedura jest procedurą, o której mowa w § 17 ust. 3 Rozporządzenia w sprawie postępowania podmiotów.
4. W zakresie przetwarzania Danych Osobowych Procedura ma pierwszeństwo przed innymi regulacjami wewnętrznymi przyjętymi przez Administratora, niedotyczącymi bezpośrednio przetwarzania Danych Osobowych.

Rozdział II.
Postanowienia szczególne

§ 3.
Podejście do realizacji obowiązków, osoby wykonujące zadania Administratora

1. Podejście do realizacji obowiązków Administratora w przedmiotowym zakresie opiera się na: wymaganiach RODO i innych przepisów powszechnie obowiązujących, rekomendacjach, opiniach i wytycznych właściwych organów nadzorczych, w tym Prezesa Urzędu Ochrony Danych Osobowych, i doradczych, w tym Grupy Roboczej Art. 29 i Europejskiej Rady Ochrony Danych.
2. Podejście, na którym oparte jest zarządzanie naruszeniami ochrony Danych Osobowych, 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. Z zastrzeżeniem postanowień szczególnych, zadania Administratora przewidziane w Procedurze wykonuje, w uzgodnieniu z Zarządem Administratora, Pracownik Administratora wyznaczony przez Zarząd. Pod nieobecność tego Pracownika lub w razie jego niewyznaczenia zadania te wykonuje samodzielnie Zarząd Administratora.
4. Zarząd ma głos decydujący w każdej sprawie. W razie powstania rozbieżności zdań co do konkretnego stanu faktycznego Zarząd przejmuje wykonywanie zadań Administratora w związku z tym konkretnym stanem faktycznym, a Pracownik, o którym mowa w ust. 3, pozostaje zobowiązany udzielać wszelkich porad i wskazówek wymaganych przez Zarząd.

§ 4.
Ustalenie powstania Incydentu

1. Pracownicy Administratora są zobowiązani zgłaszać mu wszelkie podejrzenia naruszenia RODO, innych przepisów o ochronie Danych Osobowych lub regulacji wewnętrznych dotyczących ochrony Danych Osobowych – niezwłocznie, lecz nie później niż w terminie 6 godzin od wykrycia danego zdarzenia. Zgłoszenia przyjmują formę pisemną lub formę e-mail.
2. Po uzyskaniu informacji o podejrzeniu naruszenia przepisów i regulacji, o których mowa w ust. 1, Administrator ocenia, czy dane naruszenie stanowi Incydent.
3. W razie uznania, że doszło do Incydentu, Administrator podejmuje działania, aby uzyskać i zabezpieczyć wszelkie informacje i dokumenty dotyczące danego Incydentu, w tym od Podmiotu Przetwarzającego lub Strony Trzeciej.
4. Bez względu na konieczność notyfikacji Incydentu Administrator podejmuje działania mające na celu usunięcie przyczyn Incydentu i ograniczenie jego skutków.

§ 5.
Obowiązek zgłoszenia Incydentu

1. Administrator jest zobowiązany do notyfikacji Incydentu tylko wówczas, gdy skutkuje on ryzykiem naruszenia praw lub wolności osób fizycznych, z zastrzeżeniem § 5. Ocena jest prowadzona między innymi z uwzględnieniem kontekstu przetwarzania Danych, łatwości identyfikacji Podmiotu Danych oraz okoliczności naruszenia.
2. Za Incydent, który wymaga notyfikacji, uznaje się w szczególności następujące zdarzenia:
    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.

§ 6.
Brak obowiązku zgłoszenia Incydentu

1. Incydent nie wymaga notyfikacji, jeżeli jest mało prawdopodobne, by skutkował ryzykiem naruszenia praw lub wolności osób fizycznych.
2. Za Incydent, który nie wymaga notyfikacji, uznaje się w szczególności następujące zdarzenia:
   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 zawodową lub naruszenia 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.

§ 7.
Zgłoszenie Incydentu

1. Zgłoszenie Incydentu 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.
2. Zgłoszenie Incydentu przekazywane do organu nadzorczego zawiera co najmniej informacje wskazane w Załączniku nr 1 do Procedury, zgodnie z art. 33 ust. 3 RODO. Zgłoszenie zawiera opis

charakteru Incydentu na dzień jego sporządzenia i w razie pojawienia się nowych okoliczności w sprawie, mających istotny wpływ na opisany wcześniej charakter naruszenia, zgłoszenie może i powinno być zaktualizowane.

3. 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.
Zawiadomienie Podmiotu Danych o Incydencie

1. Niezależnie od obowiązków wskazanych w § 6 Administrator jest zobowiązany do poinformowania Podmiotu Danych o Incydencie, w przypadku gdy skutkuje on wysokim ryzykiem naruszenia praw lub wolności osób fizycznych – przez co rozumie się taki Incydent, który może powodować powstanie u osoby m.in.:
   1) uszczerbku fizycznego;
   2) szkód majątkowych lub niemajątkowych, takich jak: utrata kontroli nad własnymi Danymi lub ograniczenie praw, dyskryminacja, kradzież lub sfałszowanie tożsamości;
   3) nieuprawnionego odwrócenia pseudonimizacji;
   4) naruszenia dobrego imienia;
   5) naruszenia poufności Danych Osobowych chronionych tajemnicą zawodową.
2. Ocena jest prowadzona między innymi z uwzględnieniem kontekstu przetwarzania Danych, łatwości identyfikacji Podmiotu Danych oraz okoliczności naruszenia.
3. Z zastrzeżeniem dokonania oceny ryzyka, o której mowa w ust. 1 i 2, za Incydent, który wymaga zawiadomienia Podmiotu Danych, mogą być uznane w szczególności przypadki wymienione w § 4 ust. 2.
4. Zawiadomienie Podmiotu Danych o Incydencie może być w konkretnym stanie faktycznym uzależnione od współpracy Administratora z organem nadzorczym, z uwzględnieniem wskazówek lub wytycznych przekazanych przez ten organ lub inne organy państwowe, w tym organy ścigania.
5. Zawiadomienie Podmiotu Danych o Incydencie 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 Incydent, w szczególności środki takie jak szyfrowanie lub inne środki uniemożliwiające odczyt osobom nieuprawnionym oraz dostęp do tych Danych; albo
   2) Administrator po stwierdzeniu Incydentu zastosował następcze środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności Podmiotu Danych, w tym poprzez zastosowanie odpowiednich technicznych i organizacyjnych środków ochrony; albo
   3) zawiadomienie wymagałoby niewspółmiernie wysokiego wysiłku – w takim przypadku wydawany jest publiczny komunikat, w szczególności w postaci informacji na stronie internetowej Administratora, lub zastosowany zostaje podobny środek, za pomocą którego Podmioty Danych zostają poinformowane w równie skuteczny sposób; albo
   4) zawiadomienie stanowiłoby naruszenie przepisów powszechnie obowiązującego prawa lub obowiązku ochrony Danych Osobowych innych Podmiotów Danych.
6. Z zastrzeżeniem dokonania oceny ryzyka, o której mowa w ust. 1 i 2, za Incydent, który nie wymaga zawiadomienia Podmiotu Danych, mogą być uznane w szczególności przypadki wskazane w § 5 ust. 2.
7. Termin zawiadomienia Podmiotu Danych o naruszeniu ochrony Danych Osobowych jest uzależniony od charakteru i wagi Incydentu, 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 Incydentu). Przykładowo, potrzeba zminimalizowania bezpośredniego ryzyka wystąpienia szkody u Podmiotu Danych będzie uzasadniała niezwłoczne jego poinformowanie, natomiast wdrożenie przez Administratora odpowiednich środków bezpieczeństwa przeciwko takim samym lub podobnym naruszeniom w przyszłości będzie uzasadniała późniejszą realizację obowiązku informacyjnego.

8. Zawiadomienie Podmiotu Danych o Incydencie może zostać zrealizowane w późniejszym terminie niż wskazany w ust. 7, jeżeli przepisy powszechnie obowiązującego prawa przewidują inny, określony w nich termin zawiadomienia Podmiotu Danych o Incydencie.
9. Zawiadomienie Podmiotu Danych zawiera co najmniej informacje wskazane w Załączniku nr 2 do Procedury, zgodnie z art. 34 ust. 2 RODO, podane jasnym i prostym językiem. Zawiadomienie zawiera opis charakteru Incydentu na dzień jego sporządzenia.
10. Zawiadomienie może być realizowane z wykorzystaniem kanałów zapewniających bezpieczne przekazywanie korespondencji, w tym w formie pisemnej na adres korespondencyjny lub elektronicznie przy wykorzystaniu dostępnych u Administratora technologii oraz kanałów komunikacji.
11. Jeżeli Administrator nie zawiadomił jeszcze Podmiotu Danych o Incydencie, organ nadzorczy – biorąc pod uwagę prawdopodobieństwo, że ten Incydent spowoduje wysokie ryzyko – może od niego tego zażądać lub może stwierdzić, że spełniony został jeden z warunków, o których mowa w ust. 5.

§ 9.
Rejestr Incydentów

1. W celu zapewnienia rozliczalności Administrator prowadzi rejestr wszystkich Incydentów, bez względu na obowiązek ich notyfikacji.
2. Rejestr, o którym mowa w ust. 1, jest prowadzony w formie papierowej lub elektronicznej, w taki sposób, aby w każdej chwili mógł być udostępniony organowi nadzorczemu w celu weryfikacji przestrzegania wymogów określonych w RODO.
3. W przypadku wystąpienia Incydentu Administrator dokumentuje ten fakt, wszelkie okoliczności tego naruszenia, jego ocenę, skutki oraz podjęte działania zaradcze, a także fakt notyfikacji i zawiadomienia Podmiotu Danych lub brak takiej konieczności z uzasadnieniem.

Rozdział III.
Postanowienia końcowe

§ 10.
Nadzór nad przestrzeganiem Procedury

1. Nadzór nad przestrzeganiem przez Pracowników Procedury jest sprawowany przez Zarząd.

§ 11.
Postanowienia końcowe

1. Naruszenie Procedury przez osobę zatrudnioną na podstawie umowy o pracę, regulowanej przez przepisy Kodeksu pracy, stanowi rażące naruszenie fundamentalnych obowiązków pracowniczych na podstawie art. 52 § 1 pkt 1 Kodeksu pracy i może prowadzić do nałożenia sankcji przewidzianych w Kodeksie pracy.
2. Za aktualizację Procedury odpowiada Zarząd.

Załącznik nr 1
do Procedury postępowania w przypadku naruszeń ochrony danych osobowych

[WZÓR POWIADOMIENIA O NARUSZENIU OCHRONY DANYCH OSOBOWYCH]

ZGŁOSZENIE DO ORGANU NADZORCZEGO

Nazwa administratora danych („Administrator”):
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 ……..[1]

Z poważaniem
….

[1] stosowane w przypadku opóźnienia w realizacji obowiązku zgłoszenia do organu nadzorczego

Załącznik nr 2
do Procedury postępowania w przypadku naruszeń ochrony danych osobowych

[WZÓR POWIADOMIENIA O NARUSZENIU OCHRONY DANYCH OSOBOWYCH]

ZAWIADOMIENIE OSOBY, KTÓREJ DANE DOTYCZĄ

Nazwa administratora danych („Administrator”):
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.

Niniejsze zawiadomienie zostało przygotowane przez Administratora zgodnie z wymaganiami art. 34 ust. 2 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
….

Procedura powierzania przetwarzania danych osobowych

Numer wersji	Data uchwały Zarządu
1	15 marca 2023

Spis Treści

Rozdział I.
Postanowienia ogólne

§ 1.
Definicje

Użyte w Procedurze terminy mają następujące znaczenie:

1) **Administrator** – spółka pod firmą iMercado sp z o.o.;
2) **Dane Osobowe, Dane** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; 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;
3) **Ocena** – ocena skutków planowanych operacji przetwarzania dla ochrony Danych Osobowych, o której mowa w art. 35 ust. 1 RODO;
4) **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;
5) **Podmiot Danych** – zidentyfikowana lub możliwa do zidentyfikowania osoba fizyczna;
6) **Podmiot Przetwarzający –** osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza Dane Osobowe w imieniu Administratora;
7) **Procedura –** niniejsza procedura;
8) **Pracownik –** członek Zarządu lub Rady Nadzorczej Administratora, osoba zatrudniona przez Administratora na podstawie umowy o pracę, a także każda osoba zatrudniona na podstawie

umowy zlecenia lub umowy o dzieło lub pozostająca w innym stosunku prawnym o podobnym charakterze z Administratorem;

9) **Rejestr –** rejestr czynności przetwarzania Danych Osobowych, o którym mowa w art. 30 ust. 1 RODO;

10) **Rejestr Kategorii –** rejestr kategorii czynności przetwarzania, o którym mowa w art. 30 ust. 2 RODO;

11) **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);

12) **Rozporządzenie w sprawie postępowania podmiotów** – rozporządzenie Ministra Finansów z dnia 23 marca 2017 r. w sprawie postępowania podmiotów prowadzących działalność w zakresie pośrednictwa w zbywaniu i odkupywaniu jednostek uczestnictwa oraz tytułów uczestnictwa, a także doradztwa inwestycyjnego w odniesieniu do takich instrumentów;

13) **Strona Trzecia** – osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż Podmiot Danych, Administrator, Podmiot Przetwarzający czy osoby, które – z upoważnienia Administratora lub Podmiotu Przetwarzającego – mogą przetwarzać Dane Osobowe.

§ 2.
Zakres przedmiotowy regulacji

1. Procedura określa:
   1) źródła standardów i praktyk w zakresie przetwarzania Danych;
   2) osoby wykonujące zadania Administratora;
   3) zasady powierzania przetwarzania Danych Osobowych;
   4) zasady audytowania Podmiotów Przetwarzających;
   5) postępowanie w przypadku zakończenia powierzenia przetwarzania;
   6) zasady prowadzenia rejestru Podmiotów Przetwarzających;
   7) osoby nadzorujące przestrzeganie Procedury przez Pracowników;
   8) możliwe konsekwencje naruszenia Procedury przez Pracowników;
   9) osoby odpowiedzialne za aktualizację Procedury.
2. Postanowienia Procedury stosuje się do wszystkich Pracowników Administratora, zgodnie z definicją powyżej.
3. Procedura jest procedurą, o której mowa w § 17 ust. 3 Rozporządzenia w sprawie postępowania podmiotów.
4. W zakresie przetwarzania Danych Osobowych Procedura ma pierwszeństwo przed innymi regulacjami wewnętrznymi przyjętymi przez Administratora, niedotyczącymi bezpośrednio przetwarzania Danych Osobowych.

Rozdział II.
Postanowienia szczególne

§ 3.
Podejście do realizacji obowiązków, osoby wykonujące zadania Administratora

1. Podejście do realizacji obowiązków Administratora w przedmiotowym zakresie opiera się na: wymaganiach RODO i innych przepisów powszechnie obowiązujących, rekomendacjach, opiniach i

wytycznych właściwych organów nadzorczych, w tym Prezesa Urzędu Ochrony Danych Osobowych, i doradczych, w tym Grupy Roboczej Art. 29 i Europejskiej Rady Ochrony Danych.

2. Z zastrzeżeniem postanowień szczególnych, zadania Administratora przewidziane w Procedurze wykonuje, w uzgodnieniu z Zarządem Administratora, Pracownik Administratora wyznaczony przez Zarząd. Pod nieobecność tego Pracownika lub w razie jego niewyznaczenia zadania te wykonuje samodzielnie Zarząd Administratora.
3. Zarząd ma głos decydujący w każdej sprawie. W razie powstania rozbieżności zdań co do konkretnego stanu faktycznego Zarząd przejmuje wykonywanie zadań Administratora w związku z tym konkretnym stanem faktycznym, a Pracownik, o którym mowa w ust. 2, pozostaje zobowiązany udzielać wszelkich porad i wskazówek wymaganych przez Zarząd.

§ 4.
Możliwość powierzenia przetwarzania

1. Z zastrzeżeniem przepisów odrębnych, Podmiot Przetwarzający może wykonywać czynności przetwarzania Danych Osobowych w imieniu Administratora na warunkach określonych w Procedurze.
2. Uzasadnieniem powierzenia przetwarzania może być w szczególności niewystarczające techniczne, organizacyjne lub merytoryczne przygotowanie Administratora do dokonywania określonych operacji na Danych Osobowych w ramach procesów przetwarzania bądź względy ekonomiczne.

§ 5.
Wybór Podmiotu Przetwarzającego

1. Przed powierzeniem przetwarzania Administrator ustala, czy w danym stanie faktycznym kwestia powierzenia przetwarzania jest przedmiotem regulacji przepisów szczególnych, które mogą potwierdzać dopuszczalność powierzenia przetwarzania, określać bardziej szczegółowe zasady powierzenia albo ograniczać bądź wyłączać możliwość powierzenia przetwarzania. W przypadku gdy przepisy szczególne regulują kwestie powierzenia przetwarzania, Administrator ma obowiązek stosować te przepisy.
2. Administrator może korzystać wyłącznie z usług Podmiotów Przetwarzających, posiadających wiedzę fachową, wiarygodność i zasoby, które zapewniają przestrzeganie przepisów RODO i innych przepisów dotyczących ochrony Danych Osobowych oraz zapewniają 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:
    1) stosowanie przez Podmiot Przetwarzający zatwierdzonego kodeksu RODO;
    2) stosowanie przez Podmiot Przetwarzający mechanizmu certyfikacji opisanego w art. 42 RODO;
    3) posiadanie aktualnej certyfikacji na zgodność z normą ISO 27001 lub udokumentowanego innego audytu w tym obszarze np. ISAE 3000 lub 3402;
    4) świadczenie na rzecz Administratora usług, które wymagają zezwolenia Komisji Nadzoru Finansowego.
3. 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).
4. W przypadku gdy Podmiot Przetwarzający, któremu Administrator zamierza powierzyć przetwarzanie Danych, nie jest w stanie spełnić wymogów dotyczących ochrony Danych określonych w RODO i innych przepisach dotyczących ochrony Danych Osobowych, powierzenie przetwarzania Danych takiemu Podmiotowi Przetwarzającemu jest niedopuszczalne.

§ 6.
Powierzenie przetwarzania

1. Powierzenie Danych do przetwarzania przez Podmiot Przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii Europejskiej lub prawu państwa członkowskiego, wiążą Podmiot Przetwarzający i Administratora i są zgodne w szczególności z art. 28 RODO. Administrator może w tym celu posłużyć się standardowymi klauzulami umownymi, przyjętymi przez Komisję Europejską lub organ nadzorczy na podstawie odpowiednio art. 28 ust. 7 i 8 RODO, o ile takowe zostaną przyjęte i uznane przez Administratora za wystarczające w danym stanie faktycznym.
2. Umowa lub inny instrument prawny jest zawierany jednocześnie z umową główną i wchodzi w życie w tym samym czasie, co umowa główna.
3. Podmiot Przetwarzający przetwarza Dane w zakresie (celach i sposobach) wskazanym umową lub innym instrumentem prawnym. W przypadku gdy Podmiot Przetwarzający narusza wskazany zakres powierzenia, uznaje się go za Administratora w zakresie wykraczającym poza wskazany zakres powierzenia.
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.

§ 7.
Audyt

1. W celu zapewnienia zgodności przetwarzania powierzonych Danych Osobowych z przepisami RODO i innych przepisów dotyczących ochrony Danych Osobowych Administrator prowadzi okresowe audyty wszystkich Podmiotów Przetwarzających, w tym w formie ankiety, a w razie powzięcia wiadomości o naruszeniu bezpieczeństwa ochrony Danych Osobowych również w formie niezwłocznej inspekcji.
2. W celu zapewnienia rozliczalności z każdego audytu sporządza się raport, zachowuje się też powiązaną dokumentację.

§ 8.
Zakończenie powierzenia przetwarzania

1. 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).

§ 9.
Rejestr

1. W celu zapewnienia rozliczalności Administrator prowadzi rejestr wszystkich Podmiotów Przetwarzających.
2. Rejestr, o którym mowa w ust. 1, jest prowadzony w formie papierowej lub elektronicznej, w taki sposób, aby w każdej chwili mógł być udostępniony organowi nadzorczemu w celu weryfikacji przestrzegania wymogów określonych w RODO.
3. W przypadku powierzenia przetwarzania Administrator odnotowuje w rejestrze, o którym mowa w ust. 1, dane Podmiotu Przetwarzającego, w tym jego dane kontaktowe, dane kontaktowe inspektora ochrony danych lub innego punktu kontaktowego, datę zawarcia i wygaśnięcia umowy lub innego instrumentu prawnego, czas trwania powierzenia, kategorie powierzonych Danych i kategorie Podmiotów Danych. Administrator dba o spójność tego rejestru z Rejestrem.

Rozdział III.
Postanowienia końcowe

§ 10.
Nadzór nad przestrzeganiem Procedury

1. Nadzór nad przestrzeganiem przez Pracowników Procedury jest sprawowany przez Zarząd.

§ 11.
Postanowienia końcowe

1. Naruszenie Procedury przez osobę zatrudnioną na podstawie umowy o pracę, regulowanej przez przepisy Kodeksu pracy, stanowi rażące naruszenie fundamentalnych obowiązków pracowniczych na podstawie art. 52 § 1 pkt 1 Kodeksu pracy i może prowadzić do nałożenia sankcji przewidzianych w Kodeksie pracy.
2. Za aktualizację Procedury odpowiada Zarząd.

Procedura prowadzenia rejestru czynności przetwarzania i rejestru kategorii czynności przetwarzania danych osobowych

Numer wersji	Data uchwały Zarządu
1	15 marca 2023

Spis Treści

Rozdział I.
Postanowienia ogólne

§ 1.
Definicje

Użyte w Procedurze terminy mają następujące znaczenie:

1) **Administrator** – spółka pod firmą iMercado sp. z o.o.;
2) **Dane Osobowe, Dane** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; 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;
3) **Ocena** – ocena skutków planowanych operacji przetwarzania dla ochrony Danych Osobowych, o której mowa w art. 35 ust. 1 RODO;
4) **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;
5) **Podmiot Danych** – zidentyfikowana lub możliwa do zidentyfikowania osoba fizyczna;
6) **Podmiot Przetwarzający –** osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza Dane Osobowe w imieniu Administratora;
7) **Procedura –** niniejsza procedura;
8) **Pracownik –** członek Zarządu lub Rady Nadzorczej Administratora, osoba zatrudniona przez Administratora na podstawie umowy o pracę, a także każda osoba zatrudniona na podstawie umowy zlecenia lub umowy o dzieło lub pozostająca w innym stosunku prawnym o podobnym charakterze z Administratorem;
9) **Rejestr –** rejestr czynności przetwarzania Danych Osobowych, o którym mowa w art. 30 ust. 1 RODO;

10) **Rejestr Kategorii –** rejestr kategorii czynności przetwarzania, o którym mowa w art. 30 ust. 2 RODO;

11) **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);

12) **Rozporządzenie w sprawie postępowania podmiotów** – rozporządzenie Ministra Finansów z dnia 23 marca 2017 r. w sprawie postępowania podmiotów prowadzących działalność w zakresie pośrednictwa w zbywaniu i odkupywaniu jednostek uczestnictwa oraz tytułów uczestnictwa, a także doradztwa inwestycyjnego w odniesieniu do takich instrumentów;

13) **Strona Trzecia** – osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż Podmiot Danych, Administrator, Podmiot Przetwarzający czy osoby, które – z upoważnienia Administratora lub Podmiotu Przetwarzającego – mogą przetwarzać Dane Osobowe.

§ 2.
Zakres przedmiotowy regulacji

1. Procedura określa:
   1) źródła standardów i praktyk w zakresie przetwarzania Danych;
   2) osoby wykonujące zadania Administratora;
   3) zasady prowadzenia przez Administratora Rejestru;
   4) przypadki, gdy Administrator prowadzi Rejestr Kategorii oraz zasady jego prowadzenia;
   5) osoby nadzorujące przestrzeganie Procedury przez Pracowników;
   6) możliwe konsekwencje naruszenia Procedury przez Pracowników;
   7) osoby odpowiedzialne za aktualizację Procedury.
2. Postanowienia Procedury stosuje się do wszystkich Pracowników Administratora, zgodnie z definicją powyżej.
3. Procedura jest procedurą, o której mowa w § 17 ust. 3 Rozporządzenia w sprawie postępowania podmiotów.
4. W zakresie przetwarzania Danych Osobowych Procedura ma pierwszeństwo przed innymi regulacjami wewnętrznymi przyjętymi przez Administratora, niedotyczącymi bezpośrednio przetwarzania Danych Osobowych.

Rozdział II.
Postanowienia szczególne

§ 3.
Podejście do realizacji obowiązków, osoby wykonujące zadania Administratora

1. Podejście do realizacji obowiązków Administratora w przedmiotowym zakresie opiera się na: wymaganiach RODO i innych przepisów powszechnie obowiązujących, rekomendacjach, opiniach i wytycznych właściwych organów nadzorczych, w tym Prezesa Urzędu Ochrony Danych Osobowych, i doradczych, w tym Grupy Roboczej Art. 29 i Europejskiej Rady Ochrony Danych.
2. Z zastrzeżeniem postanowień szczególnych, zadania Administratora przewidziane w Procedurze wykonuje, w uzgodnieniu z Zarządem Administratora, Pracownik Administratora wyznaczony przez Zarząd. Pod nieobecność tego Pracownika lub w razie jego niewyznaczenia zadania te wykonuje samodzielnie Zarząd Administratora.
3. Zarząd ma głos decydujący w każdej sprawie. W razie powstania rozbieżności zdań co do konkretnego stanu faktycznego Zarząd przejmuje wykonywanie zadań Administratora w związku z

tym konkretnym stanem faktycznym, a Pracownik, o którym mowa w ust. 2, pozostaje zobowiązany udzielać wszelkich porad i wskazówek wymaganych przez Zarząd.

§ 4.
Rejestr

1. Administrator prowadzi rejestr czynności przetwarzania Danych Osobowych, za które odpowiada.
2. Administrator zapewnia aktualność Rejestru poprzez ciągłe monitorowanie procesów przetwarzania Danych.
3. W Rejestrze zamieszcza się wszystkie następujące informacje:
   1) nazwę oraz dane kontaktowe Administratora oraz Inspektora, o ile został wyznaczony;
   2) czynności przetwarzania;
   3) jednostkę organizacyjną co do zasady odpowiedzialną za daną czynność przetwarzania, o ile Administrator wyodrębnił w swojej strukturze jednostki organizacyjne;
   4) cele przetwarzania;
   5) kategorie Podmiotów Danych;
   6) kategorie Danych Osobowych;
   7) podstawę prawną;
   8) źródło Danych;
   9) jeżeli jest to możliwe – planowany termin usunięcia kategorii Danych;
   10) nazwę oraz dane kontaktowe współadministratora;
   11) nazwę oraz dane kontaktowe Podmiotu Przetwarzającego;
   12) kategorie Odbiorców innych niż Podmiot Przetwarzający, którym Dane Osobowe zostały lub zostaną ujawnione, w tym Odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
   13) nazwę systemu lub oprogramowania stosowanego w przypadku danej czynności przetwarzania;
   14) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO;
   15) informację, czy dla danej czynności przetwarzania sporządzono ocenę skutków dla ochrony Danych, o której mowa w art. 35 ust. 1 RODO;
   16) 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;
4. Rejestr ma formę pisemną, w tym dopuszczalna jest forma elektroniczna. Rejestr jest udostępniany na każde żądanie organu nadzorczego. Z uwagi na zawarte informacje dot. zabezpieczeń Danych Rejestr powinien być traktowany jako dokument poufny – o ograniczonym dostępie.

§ 5.
Rejestr Kategorii

1. W przypadku gdy Administrator przetwarza Dane Osobowe w imieniu innego administratora, prowadzi odrębnie Rejestr Kategorii.
2. Administrator jako Podmiot Przetwarzający zapewnia aktualność Rejestru Kategorii poprzez ciągłe monitorowanie procesów przetwarzania Danych.
3. W Rejestrze Kategorii zamieszcza się wszystkie następujące informacje:

1) nazwę oraz dane kontaktowe Administratora jako Podmiotu Przetwarzającego oraz Inspektora, o ile został wyznaczony;
2) kategorie przetwarzań dokonywanych w imieniu każdego z Administratorów;
3) jeżeli jest to możliwe – ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO;
4) nazwę oraz dane kontaktowe każdego administratora, w imieniu którego Administrator działa jako Podmiot Przetwarzający, oraz inspektora ochrony danych, o ile został wyznaczony;
5) nazwę oraz dane kontaktowe każdego współadministratora lub przedstawiciela administratora – jeśli dotyczy;
6) czas trwania przetwarzania;
7) 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;
8) nazwę oraz dane kontaktowe podprzetwarzającego (podwykonawcy) oraz kategorie podpowierzonych przetwarzań.

4. Rejestr Kategorii ma formę pisemną, w tym dopuszczalna jest forma elektroniczna. Rejestr jest udostępniany na każde żądanie organu nadzorczego. Z uwagi na zawarte informacje dot. zabezpieczeń Danych Rejestr Kategorii powinien być traktowany jako dokument poufny – o ograniczonym dostępie.

Rozdział III.
Postanowienia końcowe

§ 6.
Nadzór nad przestrzeganiem Procedury

1. Nadzór nad przestrzeganiem przez Pracowników Procedury jest sprawowany przez Zarząd.

§ 7.
Postanowienia końcowe

1. Naruszenie Procedury przez osobę zatrudnioną na podstawie umowy o pracę, regulowanej przez przepisy Kodeksu pracy, stanowi rażące naruszenie fundamentalnych obowiązków pracowniczych na podstawie art. 52 § 1 pkt 1 Kodeksu pracy i może prowadzić do nałożenia sankcji przewidzianych w Kodeksie pracy.
2. Za aktualizację Procedury odpowiada Zarząd.

Procedura retencji i usuwania danych osobowych

Numer wersji	Data uchwały Zarządu
1	15 marca 2023

Spis Treści

Rozdział I.
Postanowienia ogólne

§ 1.
Definicje

Użyte w Procedurze terminy mają następujące znaczenie:

1) **Administrator** – spółka pod firmą iMercado sp. z o.o.;
2) **Dane Osobowe, Dane** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; 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;
3) **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;
4) **Podmiot Danych** – zidentyfikowana lub możliwa do zidentyfikowania osoba fizyczna;
5) **Podmiot Przetwarzający –** osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza Dane Osobowe w imieniu Administratora;
6) **Procedura –** niniejsza procedura;
7) **Pracownik –** członek Zarządu lub Rady Nadzorczej Administratora, osoba zatrudniona przez Administratora na podstawie umowy o pracę, a także każda osoba zatrudniona na podstawie umowy zlecenia lub umowy o dzieło lub pozostająca w innym stosunku prawnym o podobnym charakterze z Administratorem;
8) **Rejestr –** rejestr czynności przetwarzania Danych Osobowych, o którym mowa w art. 30 ust. 1 RODO;
9) **Rejestr Kategorii –** rejestr kategorii czynności przetwarzania, o którym mowa w art. 30 ust. 2 RODO;
10) **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);

11) **Rozporządzenie w sprawie postępowania podmiotów** – rozporządzenie Ministra Finansów z dnia 23 marca 2017 r. w sprawie postępowania podmiotów prowadzących działalność w zakresie pośrednictwa w zbywaniu i odkupywaniu jednostek uczestnictwa oraz tytułów uczestnictwa, a także doradztwa inwestycyjnego w odniesieniu do takich instrumentów;

12) **Strona Trzecia** – osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż Podmiot Danych, Administrator, Podmiot Przetwarzający czy osoby, które – z upoważnienia Administratora lub Podmiotu Przetwarzającego – mogą przetwarzać Dane Osobowe.

§ 2.
Zakres przedmiotowy regulacji

1. Procedura określa:
   1) źródła standardów i praktyk w zakresie przetwarzania Danych;
   2) osoby wykonujące zadania Administratora;
   3) zasady przechowywania i usuwania Danych Osobowych;
   4) osoby nadzorujące przestrzeganie Procedury przez Pracowników;
   5) możliwe konsekwencje naruszenia Procedury przez Pracowników;
   6) osoby odpowiedzialne za aktualizację Procedury.
2. Postanowienia Procedury stosuje się do wszystkich Pracowników Administratora, zgodnie z definicją powyżej.
3. Procedura jest procedurą, o której mowa w § 17 ust. 3 Rozporządzenia w sprawie postępowania podmiotów.
4. W zakresie przetwarzania Danych Osobowych Procedura ma pierwszeństwo przed innymi regulacjami wewnętrznymi przyjętymi przez Administratora, niedotyczącymi bezpośrednio przetwarzania Danych Osobowych.

Rozdział II.
Postanowienia szczególne

§ 3.
Podejście do realizacji obowiązków, osoby wykonujące zadania Administratora

1. Podejście do realizacji obowiązków Administratora w przedmiotowym zakresie opiera się na: wymaganiach RODO i innych przepisów powszechnie obowiązujących, rekomendacjach, opiniach i wytycznych właściwych organów nadzorczych, w tym Prezesa Urzędu Ochrony Danych Osobowych, i doradczych, w tym Grupy Roboczej Art. 29 i Europejskiej Rady Ochrony Danych.
2. Z zastrzeżeniem postanowień szczególnych, zadania Administratora przewidziane w Procedurze wykonuje, w uzgodnieniu z Zarządem Administratora, Pracownik Administratora wyznaczony przez Zarząd. Pod nieobecność tego Pracownika lub w razie jego niewyznaczenia zadania te wykonuje samodzielnie Zarząd Administratora.
3. Zarząd ma głos decydujący w każdej sprawie. W razie powstania rozbieżności zdań co do konkretnego stanu faktycznego Zarząd przejmuje wykonywanie zadań Administratora w związku z tym konkretnym stanem faktycznym, a Pracownik, o którym mowa w ust. 2, pozostaje zobowiązany udzielać wszelkich porad i wskazówek wymaganych przez Zarząd.

§ 4.
Zasady przechowywania i usuwania Danych

1. Dane Osobowe nie mogą być przechowywane w formie umożliwiającej identyfikację Podmiotu Danych przez okres dłuższy, niż jest to niezbędne do realizacji celów, w których Dane zostały zebrane. Cele i okres retencji Danych są każdorazowo wskazywane odpowiednio w Rejestrze lub Rejestrze Kategorii. Wskazanie okresu retencji Danych może mieć charakter opisowy, ale umożliwiający w każdym przypadku indywidualne ustalenie jego długości.
2. Z zastrzeżeniem realizacji przez Podmioty Danych praw, o których mowa w art. 17, 18 i 21 RODO, po osiągnięciu zamierzonych celów przetwarzania Dane Osobowe Podmiotów Danych powinny zostać usunięte lub zanonimizowane, chyba że ich dalsze przetwarzanie, w tym przechowywanie, znajduje podstawę prawną.
3. Dalsze przetwarzanie Danych Osobowych jest dopuszczalne m.in. w celu:
    1) archiwalnym (cywilnoprawnym) dla zabezpieczenia się przed roszczeniami Podmiotów Danych do czasu ich przedawnienia w związku ze świadczoną usługą – Dane przechowujemy przez okres przedawnienia możliwego do podniesienia roszczenia, powiązanego z tymi Danymi, a jeśli roszczenie zostało stwierdzone prawomocnym orzeczeniem sądu lub innego organu powołanego do rozpoznawania spraw danego rodzaju albo orzeczeniem sądu polubownego, jak również ugodą zawartą przed sądem albo przed sądem polubownym, albo ugodą zawartą przed mediatorem i zatwierdzoną przez sąd – odpowiednio 10 lat od tego zdarzenia, chociażby termin przedawnienia roszczeń tego rodzaju był krótszy, albo 3 lata od tego zdarzenia, jeżeli stwierdzone w ten sposób roszczenie obejmuje świadczenia okresowe; w obu przypadkach dodatkowo przez 5 lat od początku roku następującego po roku obrotowym, w którym upłynął wskazany termin odpowiednio 10 lat albo 3 lat;
    2) archiwalnym (karnoprawnym) dla zabezpieczenia się przed odpowiedzialnością Administratora jako podmiotu zbiorowego na gruncie ustawy z dnia 28 października 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary w zw. z art. 101 i 102 ustawy z dnia 6 czerwca 1997 r. Kodeks karny;
    3) ciągłego i niezakłóconego prowadzenia działalności poprzez zapewnienie integralności kopii archiwalnych lub awaryjnych od momentu ich utworzenia aż do likwidacji;
    4) realizacji zadań przez instytucje obowiązane w związku z przeciwdziałaniem praniu pieniędzy oraz finansowaniu terroryzmu;
    5) realizacji przepisów dotyczących implementacji MIFID.
4. Administrator może przechowywać Dane 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 na mocy art. 89 ust. 1 RODO, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy RODO 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.
7. Jeśli Administrator zleca zniszczenie lub anonimizację Danych innemu podmiotowi (podwykonawcy), podjęcie przez ten podmiot czynności w ramach zlecenie jest poprzedzone zawarciem z Administratorem umowy powierzenia przetwarzania Danych.

Rozdział III.
Postanowienia końcowe

§ 5.
Nadzór nad przestrzeganiem Procedury

1. Nadzór nad przestrzeganiem przez Pracowników Procedury jest sprawowany przez Zarząd.

§ 6.
Postanowienia końcowe

1. Naruszenie Procedury przez osobę zatrudnioną na podstawie umowy o pracę, regulowanej przez przepisy Kodeksu pracy, stanowi rażące naruszenie fundamentalnych obowiązków pracowniczych na podstawie art. 52 § 1 pkt 1 Kodeksu pracy i może prowadzić do nałożenia sankcji przewidzianych w Kodeksie pracy.
2. Za aktualizację Procedury odpowiada Zarząd.

Procedura zautomatyzowanego podejmowania decyzji, w tym profilowania

Numer wersji	Data uchwały Zarządu
1	15 marca 2023

Spis Treści

Rozdział I.
Postanowienia ogólne

§ 1.
Definicje

Użyte w Procedurze terminy mają następujące znaczenie:

1) **Administrator** – spółka pod firmą iMercado sp. z o.o.;
2) **Dane Osobowe, Dane** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; 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;
3) **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;
4) **Ocena** – ocena skutków planowanych operacji przetwarzania dla ochrony Danych Osobowych, o której mowa w art. 35 ust. 1 RODO;
5) **Podmiot Danych** – zidentyfikowana lub możliwa do zidentyfikowania osoba fizyczna;
6) **Podmiot Przetwarzający** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza Dane Osobowe w imieniu Administratora;
7) **Procedura** – niniejsza procedura;
8) **Pracownik** – członek Zarządu lub Rady Nadzorczej Administratora, osoba zatrudniona przez Administratora na podstawie umowy o pracę, a także każda osoba zatrudniona na podstawie umowy zlecenia lub umowy o dzieło lub pozostająca w innym stosunku prawnym o podobnym charakterze z Administratorem;
9) **Rejestr** – rejestr czynności przetwarzania Danych Osobowych, o którym mowa w art. 30 ust. 1 RODO;
10) **Rejestr Kategorii** – rejestr kategorii czynności przetwarzania, o którym mowa w art. 30 ust. 2 RODO;

11) **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);

12) **Rozporządzenie w sprawie postępowania podmiotów** – rozporządzenie Ministra Finansów z dnia 23 marca 2017 r. w sprawie postępowania podmiotów prowadzących działalność w zakresie pośrednictwa w zbywaniu i odkupywaniu jednostek uczestnictwa oraz tytułów uczestnictwa, a także doradztwa inwestycyjnego w odniesieniu do takich instrumentów;

13) **Strona Trzecia** – osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż Podmiot Danych, Administrator, Podmiot Przetwarzający czy osoby, które – z upoważnienia Administratora lub Podmiotu Przetwarzającego – mogą przetwarzać Dane Osobowe.

§ 2.
Zakres przedmiotowy regulacji

1. Procedura określa:
   1) źródła standardów i praktyk w zakresie przetwarzania Danych;
   2) osoby wykonujące zadania Administratora;
   3) zakaz zautomatyzowanego podejmowania decyzji w określonych przypadkach i wyjątki od tego zakazu;
   4) osoby nadzorujące przestrzeganie Procedury przez Pracowników;
   5) możliwe konsekwencje naruszenia Procedury przez Pracowników;
   6) osoby odpowiedzialne za aktualizację Procedury.
2. Postanowienia Procedury stosuje się do wszystkich Pracowników Administratora, zgodnie z definicją powyżej.
3. Procedura jest procedurą, o której mowa w § 17 ust. 3 Rozporządzenia w sprawie postępowania podmiotów.
4. W zakresie przetwarzania Danych Osobowych Procedura ma pierwszeństwo przed innymi regulacjami wewnętrznymi przyjętymi przez Administratora, niedotyczącymi bezpośrednio przetwarzania Danych Osobowych.

Rozdział II.
Postanowienia szczególne

§ 3.
Podejście do realizacji obowiązków, osoby wykonujące zadania Administratora

1. Podejście do realizacji obowiązków Administratora w przedmiotowym zakresie opiera się na: wymaganiach RODO i innych przepisów powszechnie obowiązujących, rekomendacjach, opiniach i wytycznych właściwych organów nadzorczych, w tym Prezesa Urzędu Ochrony Danych Osobowych, i doradczych, w tym Grupy Roboczej Art. 29 i Europejskiej Rady Ochrony Danych.
2. Z zastrzeżeniem postanowień szczególnych, zadania Administratora przewidziane w Procedurze wykonuje, w uzgodnieniu z Zarządem Administratora, Pracownik Administratora wyznaczony przez Zarząd. Pod nieobecność tego Pracownika lub w razie jego niewyznaczenia zadania te wykonuje samodzielnie Zarząd Administratora.
3. Zarząd ma głos decydujący w każdej sprawie. W razie powstania rozbieżności zdań co do konkretnego stanu faktycznego Zarząd przejmuje wykonywanie zadań Administratora w związku z tym konkretnym stanem faktycznym, a Pracownik, o którym mowa w ust. 2, pozostaje zobowiązany udzielać wszelkich porad i wskazówek wymaganych przez Zarząd.

§ 4.
Zakaz i wyjątki od zakazu

1. Podmiot Danych ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec niego skutki prawne lub w podobny sposób istotnie na niego wpływa.
2. Dozwolone jest podejmowanie wobec Podmiotu Danych decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, jeśli taka decyzja nie wywołuje wobec Podmiotu Danych skutków prawnych ani nie wpływa na niego w istotny sposób.
3. Zakaz, o którym mowa w ust. 1, nie ma zastosowania, jeżeli decyzja:
   1) jest niezbędna do zawarcia lub wykonania umowy między Podmiotem Danych a Administratorem; lub
   2) jest dozwolona prawem Unii Europejskiej lub prawem państwa członkowskiego, któremu podlega Administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub
   3) opiera się na wyraźnej zgodzie Podmiotu Danych.
4. W przypadkach, o których mowa w ust. 3 lit. a) i c), Administrator wdraża właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów Podmiotu Danych, a co najmniej prawa do uzyskania interwencji ludzkiej ze strony Administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji.
5. Decyzje, o których mowa w ust. 3, nie mogą opierać się na szczególnych kategoriach danych osobowych, o których mowa w art. 9 ust. 1 RODO, chyba że zastosowanie ma art. 9 ust. 2 lit. a) lub g) RODO i istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą.
6. W przypadku gdy Administrator 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 ust. 1.

Rozdział III.
Postanowienia końcowe

§ 5.
Nadzór nad przestrzeganiem Procedury

1. Nadzór nad przestrzeganiem przez Pracowników Procedury jest sprawowany przez Zarząd.

§ 6.
Postanowienia końcowe

1. Naruszenie zakazu, o którym mowa w § 4 ust. 1 Procedury, przez osobę zatrudnioną na podstawie umowy o pracę, regulowanej przez przepisy Kodeksu pracy, stanowi rażące naruszenie fundamentalnych obowiązków pracowniczych na podstawie art. 52 § 1 pkt 1 Kodeksu pracy i może prowadzić do nałożenia sankcji przewidzianych w Kodeksie pracy.
2. Za aktualizację Procedury odpowiada Zarząd.

REGULAMIN
FUNKCJONOWANIA INSPEKTORA OCHRONY DANYCH
W IMERCADO SP. Z O.O.

Numer wersji	Data uchwały Zarządu
1	

ROZDZIAŁ I
POSTANOWIENIA OGÓLNE

§ 1. Definicje

Użyte w Regulaminie terminy mają następujące znaczenie:

1) **Administrator** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania; na gruncie niniejszego Regulaminu Administratorem jest Spółka;
2) **Inspektor Ochrony Danych, IOD** – Inspektor Ochrony Danych w Spółka;
3) **Pracownik** – członek Zarządu Spółki, osoba zatrudniona przez Spółkę na podstawie umowy o pracę, a także każda osoba zatrudniona na podstawie umowy zlecenia lub umowy o dzieło lub pozostająca w innym stosunku prawnym o podobnym charakterze ze Spółką;
4) **Regulamin** – niniejszy Regulamin
5) **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)
6) **Rozporządzenie w sprawie postępowania podmiotów prowadzących działalność w zakresie pośrednictwa w zbywaniu i odkupywaniu jednostek uczestnictwa** – rozporządzenie Ministra Rozwoju i Finansów z dnia 23 marca 2017 r. w sprawie postępowania podmiotów prowadzących działalność w zakresie pośrednictwa w zbywaniu i odkupywaniu jednostek uczestnictwa oraz tytułów uczestnictwa, a także doradztwa inwestycyjnego w odniesieniu do takich instrumentów;
7) **SPÓŁKA –** iMercado spółka z ograniczoną odpowiedzialnością;

§ 2. Zakres przedmiotowy regulacji

1. Niniejszy Regulamin określa:
   1) zasady wyznaczania IOD;
   2) status IOD w Spółce;
   3) zadania IOD;
   4) uprawnienia IOD;
   5) sankcje za naruszenie postanowień Regulaminu.
2. Przepisy Regulaminu stosuje się do wszystkich Pracowników Spółki, zgodnie z definicją powyżej.
3. Regulamin jest procedurą, o której mowa w § 16 ust. 1 Rozporządzenia w sprawie postępowania podmiotów prowadzących działalność w zakresie pośrednictwa w zbywaniu i odkupywaniu jednostek uczestnictwa.

ROZDZIAŁ II
ZASADY WYZNACZANIA IOD

§ 3. Obowiązek wyznaczenia IOD

1. Administrator wyznacza IOD, zawsze gdy:
   1) przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;
   2) główna działalność Administratora polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę; lub
   3) główna działalność Administratora polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10 RODO.

2. Wyznaczenie IOD dla Spółki nie jest obligatoryjne z uwagi na ust. 1 powyżej, ale jest zasadne, ponieważ główna działalność Spółki polega na operacjach przetwarzania danych osobowych na dużą skalę.

§ 4. Wymagania wobec kandydata na IOD

1. IOD jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w § 8 Regulaminu.
2. IOD powinien mieć ukończone studia magisterskie na kierunku prawo oraz posiadać odpowiednią wiedzę z zakresu krajowych i europejskich przepisów o ochronie danych osobowych i praktyk jak również dogłębną znajomość RODO.
3. Niezbędny poziom wiedzy fachowej należy ustalić w szczególności w świetle prowadzonych operacji przetwarzania danych oraz ochrony, której wymagają przetwarzane dane osobowe. Wymagany poziom wiedzy fachowej musi być współmierny do charakteru, skomplikowania i ilości danych przetwarzanych w ramach Spółki.
4. IOD powinien ponadto posiadać wiedzę na temat danego sektora, a także operacji przetwarzania danych, systemów informatycznych oraz zabezpieczeń stosowanych w Spółce i jej potrzeb w zakresie ochrony danych.

§ 5. Umowa z IOD

Funkcja IOD może być pełniona na podstawie umowy o pracę, umowy zlecenie lub umowy o świadczenie usług.

§ 6. Łączenie funkcji

1. IOD może wykonywać inne zadania i obowiązki, o ile nie powoduje to konfliktu interesów. Konflikt interesów powstaje w sytuacji zajmowania w Spółce stanowiska pociągającego za sobą określanie sposobów i celów przetwarzania danych.
2. Konflikt interesów nie zachodzi w sytuacji jednoczesnego zajmowania w Spółce stanowiska doradczego, np.: prawnik, risk manager.
3. Konflikt interesów zachodzi w sytuacji jednoczesnego zajmowania w Spółce następujących stanowisk:
   1) Członek Zarządu;
   2) Dyrektor Departamentu, jeśli bierze udział w określaniu celów i sposobów przetwarzania danych;
   3) Pracownik niższego szczebla, jeśli bierze udział w określaniu celów i sposobów przetwarzania danych.

ROZDZIAŁ III
STATUS IOD W SPÓŁKA

§ 7. Status IOD

1. Spółka zapewnia, by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.
2. Spółka wspiera IOD w wypełnianiu przez niego zadań, o których mowa w § 8 Regulaminu, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.
3. IOD podlega bezpośrednio i raportuje do Zarządu Spółki.
4. IOD nie otrzymuje instrukcji dotyczących wykonywania swoich zadań.
5. IOD nie jest odwoływany ani karany przez Spółkę za wykonywanie swoich zadań.
6. Osoby, których dane dotyczą, mogą kontaktować się z IOD we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.

7. Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań - zgodnie z prawem Unii lub prawem państwa członkowskiego.

ROZDZIAŁ IV
ZADANIA I UPRAWNIENIA IOD

§ 8. Zadania IOD

1. IOD ma następujące zadania:
   1) informowanie Spółki oraz Pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
   2) monitorowanie przestrzegania RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk Spółki w dziedzinie ochrony danych osobowych, w tym: podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
   3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
   4) współpraca z publicznym organem nadzoru nad ochroną danych osobowych;
   5) pełnienie funkcji punktu kontaktowego dla publicznego organu nadzoru nad ochroną danych osobowych w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.
2. Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

§ 9. Uprawnienia IOD

3. W celu zapewnienia właściwego poziomu ochrony przetwarzanych danych IOD może:
   1) zbierać informacje w celu identyfikacji procesów przetwarzania, na co składa się m.in.: prawo wstępu do wszystkich pomieszczeń zajmowanych przez Pracowników, prawo wglądu we wszelkie dokumenty oraz prawo zapoznania się ze wszelkimi danymi zapisanymi na innych nośnikach informacji związanymi z czynnościami wykonywanymi przez danego Pracownika, prawo żądania od Pracowników jednostek kontrolowanych ustnych lub pisemnych wyjaśnień;
   2) analizować i sprawdzać zgodność przetwarzania z prawem;
   3) informować, doradzać i rekomendować określone działania Spółki i jego Pracownikom.

§ 10. Nadzór nad przestrzeganiem Regulaminu

1. Nadzór nad przestrzeganiem w Spółce przez Pracowników Regulaminu jest sprawowany przez Zarząd.
2. Wszystkie jednostki organizacyjne Spółki są zobowiązane do codziennej współpracy z IOD, polegającej m.in. na udostępnianiu IOD wszelkich dokumentów i nośników informacji, jak również zapewnieniu IOD dostępu do wszystkich pomieszczeń Spółki.

ROZDZIAŁ V
§ 11. Postanowienia Końcowe

1. Nieuprawniona odmowa wykonania polecenia IOD, w szczególności dot. przekazania informacji, przez osobę zatrudnioną na podstawie umowy o pracę, regulowanej przez przepisy Kodeksu pracy, stanowi rażące naruszenie fundamentalnych obowiązków pracowniczych na podstawie art. 52 § 1 pkt 1 Kodeksu pracy i może prowadzić do nałożenia sankcji przewidzianych w Kodeksie pracy.
2. Za aktualizację Regulaminu odpowiada Zarząd.