POLITYKA OCHRONY

DANYCH OSOBOWYCH

(POLITYKA PRYWATNOŚCI)

PAMEX Władysław Michalak

§ 1

DEKLARACJA I ZASTOSOWANIE

1. **Celem** niniejszej Polityki ochrony danych osobowych (PODO) jest wypełnienie założeń Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, dalej też zwane RODO).
2. Stanowi ona zbiór wymogów, zasad i regulacji ochrony danych osobowych u **Administratora Danych Osobowych**, którym jest **Władysław Michalak, prowadzący działalność gospodarczą pod nazwą PAMEX Władysław Michalak, zamieszkały w Żłobiźnie, ul. Brzeska 77, 49 – 305 Brzeg, NIP: 7470002477, REGON: 530504552** - dalej jako ADO.
3. Zasady, działania, kompetencje i zakresy odpowiedzialności opisane w niniejszej Polityce Ochrony Danych Osobowych (PODO lub Polityka), obowiązują wszystkich pracowników, współpracowników, zleceniobiorców, wykonawców i podwykonawców ADO.
4. Procedury i dokumenty związane z Polityką będą weryfikowane i dostosowywane w celu zapewnienia odpowiedniego poziomu bezpieczeństwa. Przeglądy dokumentacji odbywają się nie rzadziej niż raz w roku.
5. Polityka określa środki techniczne i organizacyjne zastosowane przez ADO dla zapewnienia ochrony danych oraz tryb postępowania w przypadku stwierdzenia naruszenia zabezpieczenia danych w systemie informatycznym lub w kartotekach papierowych, albo w sytuacji podejrzenia o takim naruszeniu.
6. Polityka została opracowana z uwzględnieniem metod i środków ochrony danych, których skuteczność w czasie ich zastosowania jest powszechnie uznawana. Za priorytet uznano zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania właściwej ochrony wraz z zachowaniem ich integralności i rozliczalności, ze szczególnym uwzględnieniem obowiązujących przepisów prawa dotyczących ochrony danych osobowych.
7. Zakres obowiązywania dokumentu.
    1) Niniejsza Polityka obowiązuje wszystkich pracowników, współpracowników, a także kontrahentów ADO.
    2) Każdy z pracowników i współpracowników ma obowiązek zapoznania się z treścią niniejszej Polityki.
    3) Polityka dotyczy wyposażenia, systemów, urządzeń przetwarzających informacje w formie elektronicznej, papierowej lub jakiejkolwiek innej.
    4) Nieprzestrzeganie postanowień zawartych w Polityce może skutkować sankcjami w pełnym zakresie dopuszczonym przez stosunek pracy oraz obowiązujące przepisy prawa.

§ 2

DEFINICJE

Administrator oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.
bezpieczeństwo informacji - zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność**;**
dane osobowe - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

dane szczególne oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej;
dane dotyczące zdrowia - oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej - w tym o korzystaniu z usług opieki zdrowotnej - ujawniające informacje o stanie jej zdrowia;
eksport danych oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej;
hasło - rozumie się przez to ciąg znaków alfanumerycznych, znany jedynie użytkownikowi;
identyfikator - rozumie się przez to, ciąg znaków literowych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
incydent ochrony danych osobowych - zdarzenie albo seria niepożądanych lub niespodziewanych zdarzeń ochrony danych osobowych stwarzających znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrożenia ochrony danych osobowych;
naruszenie ochrony danych osobowych - oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
obszar przetwarzania danych - rozumie się przez to budynki i pomieszczenia określone przez administratora danych, tworzące obszar, w którym przetwarzane są dane osobowe i inne informacje prawem chronione;
odbiorca danych - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią; organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania**;**
osoba, podmiot danych - oznacza osobę, której dane dotyczą;
podmiot przetwarzający - oznacza organizację lub osobę, której ADO powierzył przetwarzanie danych osobowych (np. usługodawca IT, dostawca ESOK czy innego systemu informatycznego);
polityka oznacza niniejszą politykę ochrony danych osobowych;
poufność danych - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
RCPDO lub rejestr oznacza rejestr czynności przetwarzania danych osobowych;
RODO oznacza rozporządzenie parlamentu europejskiego i rady (UE) 2016/679 z 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) (dz.urz. UE l 119, s. 1).
ryzyko - niepewność osiągnięcia zamierzonych celów**;**
system informatyczny administratora danych - rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych;
szacowanie ryzyka - proces identyfikowania, analizowania i oceniania ryzyka;
Teczka ODO - zbiór dokumentów, instrukcji, regulaminów, załączników opisujących sposób przetwarzania i ochrony danych, składający się na politykę ochrony danych osobowych, gromadzonych i nadzorowanych przez ADO.
teletransmisja - rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
uwierzytelnienie - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

użytkownik - rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło;
zgoda osoby, której dane dotyczą 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.

§ 3

ZASADY OCHRONY DANYCH

System zarządzania ochroną danych osobowych zgodny z wymaganiami niniejszej Polityki działa z poszanowaniem następujących zasad:
1) w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
2) rzetelnie i uczciwie (rzetelność);
3) w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
4) w konkretnych celach i nie "na zapas" (minimalizacja);
5) nie więcej niż potrzeba (adekwatność);
6) z dbałością o prawidłowość danych (prawidłowość);
7) nie dłużej niż potrzeba (czasowość);
8) zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

§ 4

1. W celu zwiększenia efektywności ochrony danych osobowych dokonano połączenia różnych zabezpieczeń w sposób umożliwiający stworzenie kilku warstw ochronnych. Jest ona realizowana poprzez: zabezpieczenia fizyczne, zabezpieczenia logiczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.
2. Zastosowane zabezpieczenia mają służyć osiągnięciu poniższych celów i zapewnić:
   1) **rozliczalność** - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
   2) **integralność** - rozumie się przez to właściwość zapewniającą, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   3) **poufność** - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
   4) **integralność systemu** - rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej jak i przypadkowej.
   5) **dostępność** - gwarantuje, że osoby, które są upoważnione i którym informacje są potrzebne, mają do nich dostęp w odpowiednim miejscu i czasie.
   6) **uwierzytelnienie** - uwiarygodnienie swojej tożsamości względem systemu teleinformatycznego;
   7) **autentyczność** - właściwość zapewniająca, że tożsamość podmiotu lub procesu jest taka, jak deklarowana;
3. Cele i strategie bezpieczeństwa:
   1) zgodność z prawem,
   2) ochrona zasobów informacyjnych i innych aktywów,
   3) uzyskanie i utrzymanie odpowiednio wysokiego poziomu bezpieczeństwa zasobów, rozumiane jako zapewnienie poufności, integralności i dostępności zasobów oraz zapewnienie rozliczalności podejmowanych działań,
   4) zapewnienie ciągłości działania procesów i właściwej reakcji na incydenty,

5) zapewnienie odpowiedniego poziomu wiedzy dotyczącej ochrony danych osobowych wśród pracowników i współpracowników poprzez zapewnienie odpowiednich szkoleń.

§ 5

ODPOWIEDZIALNOŚĆ ZA BEZPIECZEŃSTWO DANYCH OSOBOWYCH

1. ADO zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez.
2. Za bezpieczeństwo danych osobowych u ADO odpowiedzialni są wszyscy pracownicy. W szczególności odpowiadają oni za przestrzeganie zasad bezpieczeństwa wynikających z niniejszej Polityki oraz zgłaszanie incydentów i naruszeń, a także wykonywanie zaleceń ADO.
3. We wszystkich umowach, które mogą dotyczyć przetwarzania danych u ADO, należy uwzględnić zapisy zobowiązujące drugą stronę do przestrzegania art. 28 RODO oraz obowiązujących przepisów krajowych.
4. ADO prowadzi rejestr podmiotów zewnętrznych, z którymi realizacja umów/porozumień/zamówień lub aneksów do nich zobowiązuje lub umożliwia zleceniobiorcy/wykonawcy dostęp do informacji zawierających dane osobowe.
5. Za przestrzeganie zasad ochrony danych osobowych i za codzienną ochronę danych odpowiedzialni są upoważnieni użytkownicy.

§ 6

Realizację zamierzeń określonych w § 3 powinny zagwarantować następujące założenia:

1) Wdrożenie procedur określających postępowanie osób dopuszczonych do przetwarzania informacji oraz ich odpowiedzialność za ochronę danych.
2) Przeszkolenie użytkowników w zakresie ochrony danych osobowych.
3) Przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację (hasła, identyfikatory).
4) Podejmowanie niezbędnych działań w celu likwidacji słabych ogniw w systemie zabezpieczeń.
5) Okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych.
6) Opracowanie procedur odtwarzania systemu w przypadku wystąpienia awarii.
7) Okresowe aktualizowanie Polityki.
8) Identyfikacja zagrożeń i analiza ryzyka.

II. OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH

§ 7

Podział zagrożeń:

1) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych.
2) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.
3) zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia, naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z

zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.

§ 8

Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są informacje to głównie:

1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
2) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy,
3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
6) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych,
7) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
8) nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,
9) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń,
10) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony informacji - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,
11) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki", itp.,
12) podmieniono lub zniszczono nośniki z danymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane,
13) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur ochrony danych osobowych (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych, itp.).

§ 9

Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.

§ 10

System ochrony danych

System ochrony danych osobowych przez ADO składa się z następujących elementów:

1) **Podstawy prawne.** ADO zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych, w tym:
   a) utrzymuje system zarządzania klauzulami dotyczącymi przetwarzania danych osobowych i komunikację na odległość,
   b) inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy Spółka przetwarza dane na podstawie prawnie uzasadnionego interesu Spółki.
2) **Obsługa praw jednostki.** ADO spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:
   a) **Obowiązki informacyjne.** ADO przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków.
   b) **Możliwość wykonania żądań.** ADO weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających.
   c) **Obsługa żądań.** ADO zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany RODO i dokumentowane.
   d) **Zawiadamianie o naruszeniach.** ADO stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.
3) **Minimalizacja.** ADO posiada zasady i metody zarządzania minimalizacją (*privacy by default*), a w tym:
   a) zasady zarządzania **adekwatnością** danych;
   b) zasady reglamentacji i zarządzania **dostępem** do danych;
   c) zasady zarządzania okresem **przechowywania** danych i weryfikacji dalszej przydatności.
4) **Bezpieczeństwo.** ADO zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:
   a) przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;
   b) przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;
   c) dostosowuje środki ochrony danych do ustalonego ryzyka;
   d) posiada system zarządzania bezpieczeństwem informacji;
   e) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych − zarządza incydentami.
5) **Przetwarzający.** ADO posiada zasady doboru przetwarzających dane na rzecz ADO, wymogów co do warunków przetwarzania (umowa powierzenia przetwarzania danych osobowych), zasad weryfikacji wykonywania umów powierzenia.
6) **Eksport danych.** ADO nie przekazuje danych do państw trzecich (czyli poza UE, Norwegię, Lichtenstein, Islandię) lub do organizacji międzynarodowych.
7) ***Privacy by design*.** ADO zarządza zmianami mającymi wpływ na prywatność. W tym celu procedury uruchamiania nowych projektów i inwestycji uwzględniają konieczność oceny wpływu zmiany na ochronę danych, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.
8) **Profilowanie**. ADO nie dokonuje profilowania przetwarzanych danych osobowych.
9) **Współadministrowanie**. ADO nie prowadzi polityki ochrony danych osobowych na zasadzie współadministrowania.

§ 11

Rejestr Czynności Przetwarzania Danych

1. RCPD stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.

2. ADO prowadzi Rejestr Czynności Przetwarzania Danych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.

3. Rejestr jest jednym z podstawowych narzędzi umożliwiających Spółce rozliczanie większości obowiązków ochrony danych.

4. W Rejestrze, dla każdej czynności przetwarzania danych, którą ADO uznał za odrębną dla potrzeb Rejestru, ADO odnotowuje co najmniej: (i) nazwę czynności, (ii) cel przetwarzania, (iii) opis kategorii osób, (iv) opis kategorii danych, (v) podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu Spółki, jeśli podstawą jest uzasadniony interes, (vi) sposób zbierania danych, (vii) opis kategorii odbiorców danych (w tym przetwarzających), (viii) ogólny opis technicznych i organizacyjnych środków ochrony danych.

5. Wzór Rejestru stanowi **Załącznik nr 1 do Polityki – „Wzór Rejestru Czynności Przetwarzania Danych".** Wzór Rejestru zawiera także kolumny nieobowiązkowe.

§ 12

Podstawy przetwarzania

1. ADO dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.

2. Wskazując ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel Spółki) ADO dookreśla podstawę w czytelny sposób, gdy jest to potrzebne.

3. ADO wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).

§ 13

Sposób obsługi praw jednostki i obowiązków informacyjnych

1. ADO dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.
2. ADO ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczenie na stronie internetowej informacji lub odwołań (linków) do informacji o prawach osób, sposobie skorzystania z nich, metodach kontaktu z ADO w tym celu.
3. ADO wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.
4. W celu realizacji praw jednostki ADO zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez ADO, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany.
5. ADO dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

§ 14

Obowiązki informacyjne

1. ADO określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.
2. ADO informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.
3. ADO informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.
4. ADO informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej.
5. ADO określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam gdzie to jest możliwe (np. tabliczka o objęciu obszaru monitoringiem wizyjnym).
6. ADO informuje osobę o planowanej zmianie celu przetwarzania danych.
7. ADO informuje osobę przed uchyleniem ograniczenia przetwarzania.
8. ADO informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).
9. ADO informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.
10. ADO bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

§ 15

Żądania osób

1. **Prawa osób trzecich**. Realizując prawa osób, których dane dotyczą, ADO wprowadza proceduralne gwarancje ochrony praw i wolności osób trzecich.
2. **Nieprzetwarzanie**. ADO informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.
3. **Odmowa**. ADO informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.
4. **Dostęp do danych**. Na żądanie osoby dotyczące dostępu do jej danych, ADO informuje osobę, czy przetwarza jej dane oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych), a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych, z zastrzeżeniem, że kopii danych wydanej w wykonaniu prawa dostępu do danych ADO nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.
5. **Kopie danych**. Na żądanie ADO wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. ADO wprowadza i utrzymuje cennik kopii danych, zgodnie z którym pobiera opłaty za kolejne kopie danych. Cena kopii danych skalkulowana jest w oparciu o oszacowany jednostkowy koszt obsługi żądania wydania kopii danych**.**
6. **Sprostowanie danych**. ADO dokonuje sprostowania nieprawidłowych danych na żądanie osoby. ADO ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych ADO informuje osobę o odbiorcach danych, na żądanie tej osoby.

7. **Uzupełnienie danych**. ADO uzupełnia i aktualizuje dane na żądanie osoby. ADO ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych**.**
8. **Usunięcie danych.** Na żądanie osoby, ADO usuwa dane, gdy:

1. dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,
2. zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,
3. osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
4. dane były przetwarzane niezgodnie z prawem,
5. konieczność usunięcia wynika z obowiązku prawnego,

9. **Ograniczenie przetwarzania.** ADO dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:
   a) osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,
   b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
   c) ADO nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
   d) osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie ADO zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

§ 16

1. **Przenoszenie danych.** Na żądanie osoby ADO wydaje w powszechnie używanym formacie nadającym się do odczytu maszynowego dane dotyczące tej osoby, które udostępniła ona ADO, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych ADO.
2. **Sprzeciw w szczególnej sytuacji.** Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Spółkę w oparciu o uzasadniony interes Spółki lub o powierzone Spółce zadanie w interesie publicznym, Spółka **uwzględni** sprzeciw, o ile nie zachodzą po stronie Spółki ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

§ 17

ADO dba o minimalizację przetwarzania danych pod kątem: (i) adekwatności danych do celów (ilości danych i zakresu przetwarzania), (ii) dostępu do danych, (iii) czasu przechowywania danych.

1. **Minimalizacja zakresu.** ADO zweryfikował zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO. ADO dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok. ADO przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą (*privacy by design*).

2. **Minimalizacja dostępu**. ADO stosuje ograniczenia dostępu do danych osobowych: prawne (zobowiązania do poufności, zakresy upoważnień), fizyczne (strefy dostępu, zamykanie pomieszczeń) i logiczne (ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe). ADO stosuje kontrolę dostępu fizycznego. ADO dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów

przetwarzających. ADO dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok. Szczegółowe zasady kontroli dostępu fizycznego i logicznego zawarte są w procedurach bezpieczeństwa fizycznego i bezpieczeństwa informacji Spółki.

3. **Minimalizacja czasu.** ADO wdraża mechanizmy kontroli danych osobowych w Spółce, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze. Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu są usuwane z systemów produkcyjnych Spółki, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez Spółkę. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

§ 18

ADO zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez ADO.

1. Analizy ryzyka i adekwatności środków bezpieczeństwa

ADO przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:

a) ADO zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania − wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.

b) ADO kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.

c) ADO przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. ADO analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

d) ADO ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania, w tym ADO ustala przydatność i stosuje takie środki i podejście jak:

(i) pseudonimizacja,

(ii) szyfrowanie danych osobowych,

(iii) inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,

(iv) środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

2. Oceny skutków dla ochrony danych

ADO dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób nie jest wysokie.

a. Środki bezpieczeństwa

ADO stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony danych.
Środki bezpieczeństwa danych osobowych stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa ADO i są bliżej opisane w procedurach przyjętych przez ADO dla tych obszarów.

b. **Zgłaszanie naruszeń**

ADO stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych w terminie 72 godzin od ustalenia naruszenia.

3. PRZETWARZAJĄCY

1. ADO posiada zasady doboru i weryfikacji przetwarzających dane na rzecz ADO opracowane w celu zapewnienia, aby przetwarzający dawali wystarczające gwarancje wdrożenia odpowiednich środków organizacyjnych i technicznych dla zapewnienia bezpieczeństwa, realizacji praw jednostki i innych obowiązków ochrony danych spoczywających na ADO.
2. ADO przyjął następujące wymagania co do umowy powierzenia przetwarzania danych stanowiące **Załącznik nr 2 do Polityki – „Wzór umowy powierzenia przetwarzania danych"**.

PRAWA PODMIOTÓW DANYCH

§ 19

Każdej osobie, której dane osobowe są przetwarzane przysługuje prawo do kontroli przetwarzania jej danych osobowych, a w szczególności prawo do:

1) uzyskania wyczerpującej informacji, czy jej dane osobowe są przetwarzane oraz do otrzymania informacji o pełnej nazwie i adresie siedziby ADO;
2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych osobowych;
3) uzyskania informacji, od kiedy są przetwarzane jej dane osobowe, oraz podania w powszechnie zrozumiałej formie treści tych danych;
4) uzyskania informacji o źródle, z którego pochodzą dane osobowe jej dotyczące;
5) uzyskania informacji o sposobie udostępniania danych osobowych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym te dane osobowe są udostępniane;
6) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem przepisów prawa albo są już zbędne do realizacji celu, dla którego zostały zebrane.

Przedstawione powyżej wzory nie stanowią katalogu zamkniętego dokumentacji składającej się na Politykę ochrony danych osobowych. Każda dodatkowa, nowa procedura, instrukcja czy wytyczna ADO dotycząca obszaru ochrony danych osobowych stanowi integralną część niniejszej Polityki, a ich dodanie nie wymaga jej zmiany.

Wypełnione załączniki przechowywane są w Teczce Ochrony Danych Osobowych.