POLITYKA BEZPIECZEŃSTWA INFORMACJI

W

POL-MAK IŁAWA SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

02 kwietnia 2021 r.

§1
CEL POWSTANIA DOKUMENTU I OŚWIADCZENIA ADMINISTRATORA DANYCH OSOBOWYCH

1. Niniejsza *Polityka bezpieczeństwa*, zwana dalej Polityką, została sporządzona i wdrożona w celu wykazania, że dane osobowe są przetwarzane i zabezpieczone zgodnie z wymogami prawa, dotyczącymi zasad przetwarzania i zabezpieczenia danych w kancelarii, w tym z Rozporządzeniem 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 (dalej jako **RODO)**.
2. Przedmiotem Polityki jest m.in. określenie, opisanie i zawarcie w niej, jak również w załączonych dokumentach:
   1) zasad przetwarzania danych osobowych,
   2) zastosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń,
   3) kategorii danych osobowych objętych ochroną, a w szczególności:
      a) zabezpieczeń danych osobowych przed ich udostępnieniem osobom nieupoważnionym,
      b) zabraniem przez osobę nieuprawnioną,
      c) przetwarzaniem z naruszeniem ustawy,
      d) zmianą, utratą, uszkodzeniem lub zniszczeniem.
3. Administratorem Danych jest POL-MAK IŁAWA SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ z siedzibą w Przeźmierowie (62 – 081) przy ul. Słonecznej 6, wpisaną do Krajowego Rejestru Sądowego, prowadzonego przez Sąd Rejonowy Poznań – Nowe Miasta i Wilda w Poznaniu, VIII Wydział Krajowego Rejestru Sądowego pod numerem KRS: 0000098499, REGON: 630421780, NIP: 7771026248 (dalej jako **ADO** lub **Administrator**).
4. Administrator nie podlega obowiązkowi powołania Inspektora Ochrony Danych Osobowych. Samodzielnie wykonuje jego zadania, zgodnie z aktualnie obowiązującymi przepisami prawa.
5. Pracownicy i współpracownicy Administratora są zobowiązani do zapoznania się z obowiązującymi procedurami i instrukcjami, a także postępowania zgodnie z nimi.

§2
DEFINICJE

1. **Administrator Danych Osobowych lub Administrator** – POL-MAK IŁAWA SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ z siedzibą w Przeźmierowie (62 – 081) przy ul. Słonecznej 6, wpisaną do Krajowego Rejestru Sądowego, prowadzonego przez Sąd Rejonowy Poznań – Nowe Miasta i Wilda w Poznaniu, VIII Wydział Krajowego Rejestru Sądowego pod numerem KRS: 0000873831, REGON: 387714113, NIP: 7812015774
2. **Dane osobowe** – wszelkie 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.
3. **Szczególne kategorie danych osobowych (dane wrażliwe)** – dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby..
4. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji narzędzi programowych zastosowanych w celu przetwarzania danych

5. **Użytkownik** – osoba upoważniona przez Administratora Danych do Przetwarzania danych osobowych. Użytkownikiem może być pracownik, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilnoprawnej.
6. **Identyfikator Użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym (Użytkownika) w razie Przetwarzania danych osobowych w takim systemie
7. **Odbiorca danych** – osoba fizyczna lub prawna, organ publiczny, jednostka 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.
8. **Osoba upoważniona** – osoba, która została upoważniona przez Administratora danych osobowych do przetwarzania danych w celu i w zakresie wskazanym w upoważnieniu. Może nią być osoba zatrudniona na podstawie umowy o pracę, umowy cywilnoprawnej, wolontariusz, stażysta, itp.
9. **Zbiór danych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
10. **Przetwarzanie danych** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
11. **Powierzenie danych** – przekazanie danych osobowych innemu podmiotowi w określonym celu i zakresie, na podstawie zawartej umowy i w ramach jej realizacji, np. umowy z biurem rachunkowym.
12. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym (Użytkownikowi) w razie przetwarzania danych osobowych w takim systemie.
13. **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu (Użytkownika) w systemach informatycznych, najczęściej polegające na wpisaniu loginu i hasła użytkownika.
14. **RODO** – oznacza Rozporządzenie Parlamentu Europejskiego i Rady EU 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Ogólne Rozporządzenie o Ochronie Danych).
15. **ASI** – to Administrator systemu informatycznego – osoba, która realizuje zadania w zakresie nadzoru nad przestrzeganiem ochrony danych osobowych w Systemie informatycznym wspierając w tym zakresie ADO lub IOD, w tym:
    1) sprawuje nadzór nad bezpieczeństwem danych osobowych w systemie informatycznym, w tym przeciwdziała dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe, oraz podejmuje odpowiednie działania w przypadku wykrycia naruszeń w systemie zabezpieczeń; nadzorowanie, o którym mowa, powinno obejmować zarządzanie kontami użytkowników (ustalenie identyfikatorów i haseł, ich przyznawanie, anulowanie, resetowanie i ochrona),
    2) dba o to, aby komputery przenośne, w których przetwarzane są dane osobowe zabezpieczone były hasłem dostępu przed nieautoryzowanym uruchomieniem oraz aby mikrokomputery te nie były udostępniane osobom nieupoważnionym do przetwarzania danych osobowych,
    3) nadzoruje naprawy, przeglądy, konserwację, likwidację urządzeń komputerowych na których zapisane są dane osobowe,

4) zarządza hasłami użytkowników i nadzoruje przestrzeganie procedur określających częstotliwości ich zmiany zgodnie z wytycznymi,
5) nadzoruje czynności związane ze sprawdzaniem systemu pod kątem obecności wirusów komputerowych, wykonywania procedur uaktualniania systemów antywirusowych i ich konfiguracji,
6) nadzoruje wykonywanie kopii awaryjnych, ich przechowywanie oraz okresowo sprawdza pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu, uaktualnia systemy służące do przetwarzania danych osobowych,
7) nadzoruje system komunikacji w sieci komputerowej oraz przesyłanie danych za pośrednictwem urządzeń teletransmisji,
8) nadzoruje funkcjonowanie mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontroluje dostęp do danych osobowych,
9) Dba o właściwe ustawienie urządzeń, tak aby minimalizować możliwość wycieku informacji.

§3
POSTANOWIENIA OGÓLNE I OBOWIĄZKI ADMINISTRATORA

1. Polityka dotyczy wszystkich danych osobowych przetwarzanych u Administratora niezależnie od formy ich przetwarzania (przetwarzane tradycyjnie zbiory ewidencyjne, systemy informatyczne) oraz od tego, czy dane są lub mogą być przetwarzane w zbiorach danych).
2. Polityka jest przechowywana w wersji elektronicznej oraz w wersji papierowej w siedzibie Administratora.
3. Polityka jest udostępniana do wglądu osobom posiadającym upoważnienie do przetwarzania danych osobowych na ich wniosek, a także osobom, którym ma zostać nadane upoważnienie do przetwarzania danych osobowych, celem zapoznania się z jej treścią.
4. Dokument Polityki, wraz z załącznikami, stanowi tajemnicę przedsiębiorstwa Administratora Danych Osobowych i jest klasyfikowany jako dokument wewnętrzny.
5. Dla skutecznej realizacji Polityki Administrator Danych zapewnia:
   1) odpowiednie do zagrożeń i kategorii danych objętych ochroną środki techniczne i rozwiązania organizacyjne,
   2) kontrolę i nadzór nad Przetwarzaniem danych osobowych,
   3) monitorowanie zastosowanych środków ochrony.
6. Monitorowanie przez Administratora zastosowanych środków ochrony obejmuje m.in. działania Użytkowników, naruszanie zasad dostępu do danych, zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi oraz wewnętrznymi.
7. Administrator zapewnia, że czynności wykonywane w związku z przetwarzaniem i zabezpieczeniem danych osobowych są zgodne z niniejszą Polityką oraz odpowiednimi przepisami prawa.
8. Realizując Politykę bezpieczeństwa informacji zapewnia się ich:
   1) poufność – informacja nie jest udostępniana lub ujawniana nieupoważnionym osobom, podmiotom i procesom,
   2) integralność – dane nie zostają zmienione lub zniszczone w sposób nie autoryzowany,
   3) dostępność – istnieje możliwość wykorzystania ich na żądanie, w założonym czasie, przez autoryzowany podmiot,
   4) rozliczalność – możliwość jednoznacznego przypisania działań poszczególnym osobom,
   5) autentyczność – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana,
   6) niezaprzeczalność – uczestnictwo w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie jest niepodważalne,
   7) niezawodność – zamierzone zachowania i skutki są spójne.

9. Każda Osoba upoważniona powinna być zapoznana z regułami oraz z kompletnymi i aktualnymi procedurami ochrony informacji w swojej jednostce organizacyjnej. Poniższe uniwersalne zasady są podstawą realizacji Polityki:
   1) Zasada uprawnionego dostępu. Każdy pracownik przeszedł szkolenie z zasad ochrony informacji, spełnia kryteria dopuszczenia do informacji i podpisał stosowne oświadczenie o zachowaniu poufności.
   2) Zasada przywilejów koniecznych. Każdy pracownik posiada prawa dostępu do informacji, ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu zadań.
   3) Zasada usług koniecznych. Wszelkie zbędne usługi są wyłączone.
   4) Zasada świadomości zbiorowej. Wszyscy pracownicy są świadomi konieczności ochrony zasobów informacyjnych Spółki i aktywnie uczestniczą w tym procesie.
   5) Zasada indywidualnej odpowiedzialności. Za bezpieczeństwo poszczególnych elementów odpowiadają konkretne osoby.
   6) Zasada obecności koniecznej. Prawo przebywania w określonych miejscach mają tylko osoby upoważnione.
   7) Zasada stałej gotowości. System jest przygotowany na wszelkie zagrożenia. Niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających bez zastosowania alternatywnych zabezpieczeń.
   8) Zasada najsłabszego ogniwa. Poziom bezpieczeństwa wyznacza najsłabszy (najmniej zabezpieczony) element.
   9) Zasada ewolucji. Każdy system musi ciągle dostosowywać mechanizmy wewnętrzne do zmieniających się warunków zewnętrznych.
   10) Zasada odpowiedniości. Używane mechanizmy muszą być adekwatne do sytuacji.
   11) Zasada akceptowanej równowagi. Podejmowane środki zaradcze nie powinny przekraczać poziomu akceptacji.
   12) Zasada świadomej konwersacji. Nie zawsze i wszędzie trzeba mówić, co się wie, ale zawsze i wszędzie trzeba wiedzieć co, gdzie i do kogo się mówi.
6. Administrator zapewnia, że:
   1) nie prowadzi przetwarzania danych, które wiązałoby się z wysokim ryzykiem naruszenia praw lub wolności osoby fizycznej,
   2) uwzględnia ochronę danych w fazie projektowania oraz stosuje domyślną politykę ochrony tam, gdzie ma to zastosowanie (tzw. „privacy by design" i „privacy by default"),
   3) respektuje prawa osoby, której dane dotyczą, w szczególności prawa dostępu do danych, sprostowania danych, bycia zapomnianym, prawo do ograniczenia przetwarzania, prawo do przenoszenia danych, prawo do sprzeciwu, zgodnie z aktualnie obowiązującymi przepisami prawa,
   4) dokona oceny skutków dla planowanych operacji przetwarzania danych osobowych przed rozpoczęciem przetwarzania – jeśli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.
10. Każde naruszenie zasad Polityki może być uznane za poważne naruszenie podstawowych obowiązków pracowniczych lub wynikających z umów cywilnoprawnych o współpracy, i może skutkować konsekwencjami i odpowiedzialnością przewidzianymi w przepisach prawnych, takich jak m.in. ustawa Kodeks pracy, ustawa Kodeks cywilny.

§4
DANE OSOBOWE PRZETWARZANE U ADMINISTRATORA DANYCH I OPIS STRUKTURY ZBIORÓW DANYCH

1. Dane osobowe przetwarzane przez Administratora gromadzone są w zbiorach danych.

2. Administrator nie podejmuje czynności przetwarzania, które mogłyby się wiązać z poważnym prawdopodobieństwem wystąpienia wysokiego ryzyka dla praw i wolności osób. W przypadku planowania takiego działania Administrator wykona czynności określone w art. 35 i nast. RODO.
3. W przypadku planowania nowych czynności przetwarzania Administrator dokonuje analizy ich skutków dla ochrony danych osobowych oraz uwzględnia kwestie ochrony danych w fazie ich projektowania. Analiza ryzyka dokonywana jest dla czynności przetwarzania występujących w każdej lokalizacji, w której Administrator prowadzi działalność.

§5
REJESTR CZYNNOŚCI PRZETWARZANIA I REJESTR KATEGORII CZYNNOŚCI PRZETWARZANIA

1. Administrator prowadzi rejestr czynności przetwarzania oraz rejestr kategorii czynności przetwarzania.
2. Administrator każdorazowo weryfikuje podstawę prawną, cel oraz zakres utworzenia nowego zbioru danych, a następnie ustala, czy przetwarzanie danych jest legalne.

§6
PODSTAWOWE ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator przetwarza dane osobowe wyłącznie, gdy jest to dopuszczone aktualnie obowiązującymi przepisami prawa.
2. Dane osobowe mogą być przetwarzane wyłącznie w celu i zakresie, w jakim zostały zgromadzone, a także nie dłużej niż jest to niezbędne dla osiągnięcia tego celu.
3. Dane osobowe po wykorzystaniu są niezwłocznie usuwane lub przechowywane wyłącznie w postaci uniemożliwiającej identyfikację osób, których dotyczą, o ile przepisy odrębnych ustaw nie podają określonego czasu przechowywania danych.
4. Dane osobowe są przetwarzane przez Administratora, m.in. gdy:
   1) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
   2) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
   3) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
   4) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
   5) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
   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 osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.
5. Administrator Danych nie przetwarza danych na teranie państwa trzeciego, ani nie powierza danych innym podmiotom poza obszarem Europejskiego Obszaru Gospodarczego.
6. Administrator Danych przetwarza szczególne kategorie danych, **tzw. dane wrażliwe**, gdy spełniony jest chociażby jeden z warunków z art. 9 ust. 2 RODO.

7. W przypadku gdy dane osobowe są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy lub są zbędne do realizacji celu, dla którego zostały zebrane, Administrator jest zobowiązany do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.
8. Administrator stosuje ogólne zasady przetwarzania danych osobowych zawarte w RODO, w szczególności w art. 5 RODO.

§7
OBOWIĄZKI I ODPOWIEDZIALNOŚĆ W ZAKRESIE ZARZĄDZANIA BEZPIECZEŃSTWEM DANYCH

1. Wszystkie osoby zobowiązane są do przetwarzania danych osobowych zgodnie z obowiązującymi przepisami i zgodnie z ustaloną przez Administratora Danych Polityką, Instrukcją Zarządzania Systemem Informatycznym, a także innymi dokumentami wewnętrznymi i procedurami związanymi z przetwarzaniem danych osobowych u Administratora.
2. Wszystkie dane osobowe u Administratora są przetwarzane z poszanowaniem zasad przetwarzania przewidzianych przez przepisy prawa:
   1) W każdym wypadku występuje chociaż jedna z przewidzianych przepisami prawa podstaw dla przetwarzania danych.
   2) Dane przetwarzane są rzetelnie i w sposób przejrzysty.
   3) Dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.
   4) Dane osobowe są przetwarzane jedynie w takim zakresie, jaki jest niezbędny dla osiągnięcia celu przetwarzania danych.
   5) Dane osobowe są prawidłowe i w razie potrzeby uaktualniane.
   6) Czas przechowywania danych jest ograniczony do okresu ich przydatności do celów, do których zostały zebrane, a po tym okresie są one anonimizowane bądź usuwane.
   7) Wobec osoby, której dane dotyczą, wykonywany jest obowiązek informacyjny zgodnie z treścią art. 13 i 14 RODO.
   8) Dane są zabezpieczone przed naruszeniami zasad ich ochrony.
3. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony Danych osobowych uważa się w szczególności:
   1) naruszenie bezpieczeństwa Systemów informatycznych, w których przetwarzane są dane osobowe, w razie ich przetwarzania w takich systemach;
   2) udostępnianie lub umożliwienie udostępniania danych osobom lub podmiotom do tego nieupoważnionym;
   3) zaniechanie, choćby nieumyślne, dopełnienia obowiązku zapewnienia danym osobowym ochrony;
   4) niedopełnienie obowiązku zachowania w tajemnicy Danych osobowych oraz sposobów ich zabezpieczenia;
   5) przetwarzanie Danych osobowych niezgodnie z założonym zakresem i celem ich zbierania;
   6) spowodowanie uszkodzenia, utraty, niekontrolowanej zmiany lub nieuprawnione kopiowanie Danych osobowych;
   7) naruszenie praw osób, których dane są przetwarzane.
4. W przypadku stwierdzenia okoliczności naruszenia zasad ochrony danych osobowych każda osoba zobowiązana jest do podjęcia wszystkich niezbędnych kroków, mających na celu ograniczenie skutków naruszenia i do niezwłocznego powiadomienia Administratora Danych.
5. Do obowiązków Administratora Danych w zakresie zatrudniania, zakończenia lub zmiany warunków zatrudnienia pracowników lub współpracowników (osób podejmujących czynności na rzecz Administratora Danych na podstawie innych umów cywilnoprawnych) należy dopilnowanie, aby:
   1) każdy z przetwarzających Dane osobowe był odpowiednio przygotowany do wykonywania swoich obowiązków,

2) każdy z przetwarzających Dane osobowe był pisemnie upoważniony do przetwarzania zgodnie z „Upoważnieniem do przetwarzania danych osobowych",

3) każdy z przetwarzających Dane osobowe zobowiązał się do zachowania danych osobowych przetwarzanych u Administratora w tajemnicy poprzez podpisanie „Oświadczenia o poufności".

6. Osoby upoważnione zobowiązane są do:
   1) ścisłego przestrzegania zakresu nadanego upoważnienia; Osoba upoważniona do przetwarzania danych osobowych może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez administratora danych w upoważnieniu i tylko w celu wykonywania nałożonych obowiązków; zakres dostępu do danych przypisany jest do niepowtarzalnego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie; rozwiązanie stosunku pracy, odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych;
   2) przetwarzania i ochrony danych osobowych zgodnie z przepisami; Osoba upoważniona do przetwarzania danych osobowych zapoznaje się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami niniejszej Polityki i Instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych;
   3) zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia; Osoba upoważniona do przetwarzania danych osobowych musi zachować tajemnicę danych osobowych oraz przestrzegać procedur ich bezpiecznego przetwarzania; przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia u administratora danych, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji; Osoba upoważniona do przetwarzania danych osobowych stosuje określone przez administratora danych oraz administratora bezpieczeństwa informacji procedury oraz wytyczne mające na celu zgodne z prawem, w tym zwłaszcza adekwatne, przetwarzanie danych;
   4) zgłaszania incydentów związanych z naruszeniem bezpieczeństwa danych oraz niewłaściwym funkcjonowaniem systemu.
7. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby, które posiadają imienne upoważnienie nadane przez Administratora Danych Osobowych.
8. Upoważnienie wydawane jest przed rozpoczęciem o przetwarzania danych osobowych na czas trwania umowy o pracę lub innej umowy cywilnoprawnej, a także na czas wykonania określonego zadania, które związane jest z przetwarzaniem danych, w celu i zakresie wynikającym z zadań i obowiązków służbowych.
9. Osoba upoważniona do przetwarzania danych osobowych składa pisemne oświadczenia o zobowiązaniu do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia.
10. Administrator Danych Osobowych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych. Ewidencja ta prowadzona jest w wersji elektronicznej, a jej wzór stanowi załącznik do Polityki.
11. Administrator Danych Osobowych aktualizuje ewidencję osób upoważnionych za każdym razem, gdy upoważnia do przetwarzania nowe osoby, zmienia zakres i cel nadanego już upoważnienia lub, gdy osoba upoważniona zakończy z nim współpracę.
12. Osoba upoważniona do przetwarzania danych jest zobowiązana do:
    1) przetwarzania danych osobowych zgodnie z upoważnieniem wydanym przez Administratora Danych Osobowych;
    2) stosowania się do instrukcji i procedur przetwarzania danych osobowych, zawartych w politykach wewnętrznych wydanych przez Administratora Danych Osobowych;
    3) stosowania wprowadzonych środków organizacyjnych i technicznych, zapewniających ochronę przetwarzania danych, w szczególności przed ich udostępnieniem, kradzieżą, uszkodzeniem lub zniszczeniem przez osoby nieupoważnione;

4) umożliwienia przeprowadzenia czynności w toku sprawdzenia planowanego lub doraźnego prowadzonego przez Administratora Danych Osobowych lub na jego zlecenie;
5) sprawowania nadzoru nad obiegiem oraz przechowywaniem i zabezpieczeniem dokumentów zawierających dane osobowe, do których ma dostęp w chwili wykonywania czynności służbowych;
6) każdorazowego niezwłocznego informowania Administratora Danych Osobowych w sytuacji naruszenia ochrony danych osobowych lub uzasadnionego podejrzenia takiego naruszenia.

§8
OBOWIĄZEK INFORMACYJNY REALIZOWANY PRZEZ ADMINISTRATORA

1. Administrator Danych Osobowych respektuje prawa, które przysługują każdej osobie, której dane dotyczą, w szczególności prawo do kontroli przetwarzania danych.
2. Administrator Danych informuje osoby, których dane dotyczą, o swoich danych, adresie, siedzibie, celu zbierania danych, obowiązku lub dobrowolności ich podania, a także przekazuje inne informacje, które mogą być wymagane aktualnie obowiązującymi przepisami prawa.
3. Obowiązek informacyjny w przypadku pozyskiwania danych bezpośrednio od osoby, której dane dotyczą wykonywany jest przed rozpoczęciem ich gromadzenia.
4. Osobę, której dane dotyczą informuje się o:
   1) dokładnej nazwie i adresie swojej siedziby;
   2) celu zbierania danych;
   3) dobrowolności lub obowiązku podania danych, a jeżeli taki obowiązek istnieje o jego podstawie prawnej;
   4) prawie wglądu do treści swoich danych oraz możliwości ich poprawiania;
   5) innych informacjach, wynikających z aktualnych przepisów prawa, w szczególności o:
      a) celu przetwarzania danych na podstawie interesu prawnego administratora danych,
      b) zamiarze przekazania danych do państwa trzeciego,
      c) okresie przez który dane będą przetwarzane, a gdy nie jest możliwe jego ustalenie to o kryteriach ustalenia tego okresu,
      d) prawie do żądania sprostowania, usunięcia lub ograniczenia przetwarzania,
      e) prawie do wniesienia sprzeciwu wobec przetwarzania,
      f) prawie do przenoszenia danych (jeśli przetwarzanie odbywa się na podstawie umowy lub zgody),
      g) prawie do cofnięcia zgody w dowolnym momencie (jeśli przetwarzanie odbywa się na podstawie zgody osoby), bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
      h) prawie wniesienia skargi do organu nadzorczego,
      i) profilowaniu i jego konsekwencjach, jeśli jest to zasadne.
5. Powyższych informacji nie udziela się jeśli osoba dysponuje już tymi informacjami, a Administrator będzie w stanie to wykazać lub, gdy obowiązek ich ujawnienia wynika z prawa UE lub prawa krajowego.
6. W przypadku zbierania danych osobowych nie bezpośrednio od osoby, której one dotyczą, osobę tę należy w rozsądnym terminie po pozyskaniu danych osobowych - najpóźniej w ciągu miesiąca - mając na uwadze konkretne okoliczności przetwarzania danych osobowych – poinformować dodatkowo o źródle danych i innych uprawnieniach wynikających z aktualnie obowiązujących przepisów.
7. Administrator ma również na uwadze, że każda osoba, której dane dotyczą, może wystąpić z wnioskiem o otrzymanie informacji o jej danych, które są przetwarzane w zbiorze u Administratora, zgodnie z obowiązującymi przepisami. Odpowiedź na zapytanie osoby, której dane dotyczą, jest udzielana na piśmie w terminie nieprzekraczającym miesiąca od daty wpłynięcia wniosku.

8. Wyłączenie obowiązku udzielenia odpowiedzi następuje wyłącznie w przypadkach, określonych aktualnie obowiązującymi przepisami prawa.
9. Obowiązek informacyjny realizowany jest poprzez podanie niezbędnych informacji na formularzach, umowach, w regulaminie lub kwestionariuszach osobowych.
10. Administrator, celem ochrony **tzw. danych wrażliwych,** które przetwarza, głównie danych o zdrowiu, oraz w celu zapewnienia realizacji praw podmiotów danych, wprowadza i przestrzega u siebie „Procedurę realizacji praw podmiotów danych zgodnie z RODO".

§9
UDOSTĘPNIANIE DANYCH OSOBOWYCH

1. Administrator Danych udostępnia dane osobowe przetwarzane w zbiorach danych wyłącznie osobom lub podmiotom uprawnionym do ich otrzymania na podstawie aktualnych przepisów prawnych.
2. Dane osobowe mogą być udostępniane na podstawie:
   1) wniosku od podmiotu uprawnionego do otrzymywania danych osobowych na podstawie przepisów prawa, w szczególności wniosku sądu, prokuratury, policji, komornika, ZUS, Urzędu Skarbowego, itp.,
   2) wniosku innej osoby lub podmiotu, na zasadach określonych w przepisach prawa.
3. Wszystkie osoby upoważnione, które otrzymają wniosek o udostępnienie danych, zobowiązane są do przekazywania go bezpośrednio do Administratora, który podejmuje decyzję o udostępnieniu lub odmowie udostępnienia.

§10
OBSZAR PRZETWARZANIA DANYCH OSOBOWYCH

1. Obszar, w którym przetwarzane są Dane osobowe, obejmuje wszystkie pomieszczenie zlokalizowane w lokalizacjach, w których Administrator prowadzi działalność, tj.:
   1) Przeźmierowo (u. Słoneczna 6, 62-081 Przeźmierowo).
   2) Batorowo (ul. Stefana Batorego 93, 62-080 Batorowo).
   3) Iława (ul. Ziemowita, 14-200 Iława).
2. Dodatkowo obszar, w którym przetwarzane są Dane osobowe, stanowią wszystkie komputery przenośne oraz inne nośniki danych (np. pendrive'y, kalendarze, telefony komórkowe) znajdujące się poza obszarem wskazanym powyżej, na których przechowuje się nośniki informacji zawierające dane osobowe.
3. Dostęp do pomieszczenia, w którym dane osobowe są przetwarzane mogą mieć wyłącznie osoby upoważnione. Inne osoby mogą przebywać w obszarze przetwarzania danych wyłącznie pod nadzorem osoby upoważnionej.
4. Gdy nie jest możliwe nadzorowanie pracy osób nieupoważnionych w obszarze przetwarzania danych osobowych, Administrator zapewnia zabezpieczenie danych osobowych, znajdujących się w danym pomieszczeniu, w taki sposób, aby nie było możliwe zabranie, zniszczenie lub jakikolwiek dostęp do tych danych.

§11
SYSTEMY INFORMATYCZNE

Administrator danych osobowych podejmuje wszelkie uzasadnione zachowania celem należytego zabezpieczenia przetwarzania danych osobowych w systemach informatycznych. Szczegóły powyższego opisane zostały w Instrukcji zarządzania systemem informatycznym.

§12
OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

1. Administrator Danych zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych.
2. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych. Środki obejmują w szczególności:
   1) Ograniczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe, jedynie do osób odpowiednio upoważnionych. Inne osoby mogą przebywać w pomieszczeniach wykorzystywanych do przetwarzania danych jedynie w towarzystwie osoby upoważnionej.
   2) Zamykanie pomieszczeń tworzących obszar Przetwarzania danych osobowych określony w §10 na czas nieobecności pracowników, w sposób uniemożliwiający dostęp do nich osób trzecich.
   3) Wykorzystanie zamykanych szafek i/lub sejfów do zabezpieczenia dokumentów.
   4) Wykorzystanie niszczarki do skutecznego usuwania dokumentów zawierających dane osobowe.
   5) Ochronę sieci lokalnej przed działaniami inicjowanymi z zewnątrz przy użyciu sieci firewall.
   6) Wykonywanie kopii awaryjnych danych.
   7) Ochronę sprzętu komputerowego wykorzystywanego u Administratora przed złośliwym oprogramowaniem.
   8) Zabezpieczenie dostępu do urządzeń salonu przy pomocy haseł dostępu.
   9) Wykorzystanie szyfrowania danych przy ich transmisji.

§13
NARUSZENIA ZASAD OCHRONY DANYCH OSOBOWYCH

1. W przypadku stwierdzenia naruszenia ochrony danych osobowych Administrator dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych.
2. W każdej sytuacji, w której zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych, Administrator zgłasza fakt naruszenia zasad ochrony danych organowi nadzorczemu bez zbędnej zwłoki – jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia.
3. Jeżeli ryzyko naruszenia praw i wolności jest wysokie, Administrator zawiadamia o incydencie także osobę, której dane dotyczą.
4. Poinformowania o naruszeniu organu nadzorczego i osoby, której dane dotyczą nie stosuje się, jeśli przepisy prawa krajowego wyłączają odpowiedzialność Administratora w tym zakresie.
5. Naruszenia nie zgłasza się organowi nadzorczemu, ani osobie, której dane dotyczą, jeśli Administrator jest w stanie wykazać małe prawdopodobieństwo naruszenia praw lub wolności osób fizycznych.
6. Wszystkie osoby upoważnione do przetwarzania danych osobowych są zobowiązane poinformować Administratora o ewentualnych naruszeniach bezpieczeństwa ochrony danych osobowych lub uzasadnionych podejrzeniach wystąpienia takiego naruszenia.
7. W przypadku jakiegokolwiek naruszenia ochrony danych osobowych Administrator sprawdza, dlaczego doszło do naruszenia i jakie środki zapobiegawcze wprowadzić.
8. Szczegółowe zasady postępowania zawierają:

§14
POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej zgodnie z wymogami wskazanymi dla takich umów w art. 28 RODO, lub poprzez akceptację regulaminu świadczonej

usługi pomiędzy Administratorem a podmiotem trzecim, któremu dane się powierza w celu i w zakresie wykonania konkretnej czynności w imieniu Administratora.

2. Przed powierzeniem przetwarzania danych osobowych Administrator w miarę możliwości uzyskuje informacje o dotychczasowych praktykach procesora dotyczących zabezpieczenia danych osobowych.
3. Administrator powierza przetwarzane dane osobowe osób fizycznych, w szczególności w celu: prowadzenia obsługi księgowej, prowadzenia obsługi prawnej, Serwisu i konserwacji urządzeń, na których znajdują się dane osobowe, usługi IT, administrowanie serwerem, hosting.
4. Umowa powierzenia określa w szczególności cel i zakres powierzenia przetwarzania danych osobowych.
5. Administrator sprawuje kontrolę nad tym w jakim zakresie i w jakim celu powierza dane osobowe. Prowadzi w tym celu ewidencję podmiotów, którym dane zostały powierzone do przetwarzania.
6. Administrator powierza dane osobowe tylko tym podmiotom, które gwarantują zastosowanie środków organizacyjnych i technicznych, zabezpieczających dane przed dostępem osób nieupoważnionych na zasadach określonych w przepisach prawa.

§15
PRZEKAZYWANIE DANYCH DO PAŃSTWA TRZECIEGO

Administrator Danych Osobowych nie będzie przekazywał danych osobowych do państwa trzeciego, poza sytuacjami w których następuje to na wniosek osoby, której dane dotyczą.

§16
POSTANOWIENIA KOŃCOWE

1. Wszyscy pracownicy, współpracownicy i osoby upoważnione do przetwarzania danych osobowych w imieniu Administratora są zobowiązani do zapoznania się i przestrzegania zasad, instrukcji i procedur wprowadzonej dokumentacji przetwarzania danych osobowych.
2. Za niedopełnienie obowiązków wynikających z niniejszego dokumentu osoby wymienione w ust. 1 ponoszą odpowiedzialność na podstawie Kodeksu pracy, Przepisów o ochronie danych osobowych, ustawy Kodeks karny oraz innych przepisów.
3. Dopuszcza się dokonywanie zmian w niniejszym dokumencie oraz dokumentach powiązanych tylko przez osoby upoważnione.
4. Zmiany w dokumencie Polityki oraz w załącznikach wprowadzane są w chwili pojawienia się ważnych okoliczności lub nowych przepisów prawnych, istotnych dla spójności i aktualności Polityki, bądź aktualizacji dotychczasowych przepisów dotyczących ochrony lub przetwarzania danych osobowych. Zmiany zatwierdzane są przez Administratora i podawane do wiadomości osób uczestniczących w przetwarzaniu danych osobowych poprzez publikację w intranecie lub dokumentach formalnych udostępnianych w ustalony wewnętrznie sposób.
5. Integralną część niniejszej Polityki są wymienione w jej treści dokumenty i wzory, a także inne dokumenty mające na celu ochronę danych osobowych a wdrożone przez Administratora.

Przemysław Makowiak
Członek Zarządu

Dariusz Makowiak
Członek Zarządu

Przemysław Makowiak Dariusz Makowiak