Zakłady Mleczarskie Laktopol-A Sp. z o.o.

w Łosicach ul. Czarkowskiego 8

08-200 Łosice

Polityka bezpieczeństwa i ochrony danych osobowych

Niniejszy dokument jest dowodem na zaadoptowanie i spełnianie przez Zakłady Mleczarskie Laktopol-A Sp. z o.o. w Łosicach ul. Czarkowskiego 8 08-200 Łosice wymagań Rozporządzenia Parlamentu Europejskiego i Rady UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO) z dnia 27-04-2016r.

	Stanowisko:	Imię i nazwisko:	Data:	Podpis:
Opracował	Inspektor Ochrony Danych Osobowych	Emilia Adamczyk	25-05-2018r.	
Zatwierdził	Dyrektor Zakładu	Monika Czapska-Zych	25-05-2018r.	

SPIS TREŚCI

I. POLITYKA BEZPIECZEŃSTWA I OCHRONY DANYCH OSOBOWYCH – WYMAGANIA OGÓLNE

Polityka Bezpieczeństwa Danych Osobowych jest dokumentem pełniącym rolę konstytutywną w stosunku do wszystkich innych - wydanych w tym zakresie wewnętrznych zarządzeń, procedur i instrukcji. Uzupełnieniem niniejszego dokumentu są wszelkie regulacje cytowane lub przywoływane w niniejszym dokumencie funkcjonujące w Zakładach Mleczarskich Laktopol-A Sp. z o.o. dokumenty wewnętrzne tj. procedury, regulaminy itp.

Polityka Bezpieczeństwa Danych Osobowych jest to formalny zapis zasad, według których zobowiązane są postępować osoby, posiadające dostęp do technologii organizacji i do jej zasobów informacyjnych. Polityka odnosi się całościowo do problemu zabezpieczenia danych osobowych, tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie jak i danych przetwarzanych w systemach informatycznych przy zachowaniu poufności, integralności, autentyczności, rozliczalności i dostępności informacji, przy niezawodności pracy całości systemu a w szczególności aplikacji i urządzeń zawierających, przetwarzających, przesyłających informacje podlegające ochronie.

Przedmiotem ochrony na podstawie niniejszej Polityki są dane osobowe, agregowane zarówno w systemach informatycznych, jak również na nośnikach papierowych i elektronicznych. Polityka ma zastosowanie do wszystkich danych osobowych przetwarzanych w Zakładach Mleczarskich Laktopol-A Sp. z o.o. w ramach realizowanych przez nią procesów biznesowych/ działań operacyjnych. Obowiązek ochrony danych osobowych przetwarzanych w Zakładach Mleczarskich Laktopol-A Sp. z o.o. dotyczy wszystkich osób, które mają do nich dostęp bez względu na zajmowane stanowisko oraz miejsce wykonywania pracy, jak również charakter stosunku pracy. Każda osoba, która ma mieć dostęp do danych osobowych, będzie mogła je przetwarzać wyłącznie na podstawie otrzymanego upoważnienia.

Osoby mające dostęp do danych osobowych są zobowiązane do zapoznania się z Polityką i innymi powiązanymi z nią dokumentami oraz stosowanie zawartych w nich regulacji. Polityka zachowuje zgodność z innymi wewnętrznymi regulacjami z obszaru bezpieczeństwa informacji i systemów informatycznych obowiązującymi w Zakładach Mleczarskich Laktopol-A Sp. z o.o. Nadzór nad opracowaniem i aktualizacją Polityki sprawuje Inspektor Ochrony Danych Osobowych.

II. DEKLARACJA BEZPIECZEŃSTWA I OCHRONY DANYCH OSOBOWYCH

„Deklaracja Kierownictwa Zakładów Mleczarskich "Laktopol-A" Sp. z o. o. dla zachowania bezpieczeństwa i ochrony przetwarzanych danych osobowych w ramach prowadzonej działalności”

Zakłady Mleczarskie "Laktopol-A" Sp. z o. o. wobec rosnącej wartości informacji, szczególnie danych osobowych, są świadome wagi zagrożeń związanych z procesem przetwarzania danych.
Zakłady Mleczarskie "Laktopol-A" Sp. z o. o. deklarują podejmowanie systematycznych działań celem zapobiegania zagrożeniom dla bezpieczeństwa informacji, których wystąpienie może prowadzić do utraty poufności, integralności i rozliczalności danych, a w szczególności do udostępnienia informacji osobom nieupoważnionym, uszkodzenia lub zniszczenia.

Dla gwarancji powyższej deklaracji Zakłady Mleczarskie "Laktopol-A" Sp. z o. o. dążą do osiągnięcia satysfakcjonującego poziomu bezpieczeństwa przetwarzanych informacji poprzez:

1. Potwierdzenie potrzeby ochrony informacji, a w szczególności danych przetwarzanych w systemach informatycznych.
2. Zapewnienie wsparcia dla inicjatyw z zakresu bezpieczeństwa informacji.
3. Zapewnienie zasobów potrzebnych dla wdrażania wymaganych zabezpieczeń.
4. Objęcie szczególnym nadzorem dokumentacji zawierającej dane osobowe niezależnie od formy jej sporządzania.
5. Zapewnienie działań na rzecz kształtowania świadomości pracowników co do ważności i rangi przetwarzanych danych w tym danych osobowych.

Deklaruje, iż niniejsza polityka będzie skutecznie realizowana i systematycznie weryfikowana na rzecz zapewnienia należytego poziomu ochrony przetwarzanych danych w tym systematycznego doskonalenia w tym obszarze.

III. PODSTAWY PRAWNE

Niniejszy dokument został oparty na założeniach wymagań prawnych w zakresie ochrony i bezpieczeństwa danych osobowych jakie każde przedsiębiorstwo przetwarzające dane osobowe zobowiązane jest spełniać miedzy innymi, Rozporządzenie Parlamentu Europejskiego i Rady UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO) z dnia 27-04-2016r.

IV. TERMINOLOGIA

1. **Rozporządzenie** - 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.

2. **Administrator Danych Osobowych = ADO** - Zgodnie z definicją RODO administrator danych osobowych oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych = Zakłady Mleczarskie Laktopol-A Sp. z o.o.,
3. **Dane osobowe** - oznacza informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
4. **Szczególne kategorie danych osobowych** – 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.
5. **Inspektor Ochrony Danych Osobowych** - Osoba wyznaczona przez Administratora danych na podstawie art. 37 RODO, która realizuje zadania monitorowania przestrzegania przepisów o ochronie danych osobowych w Zakładach Mleczarskich Laktopol-A Sp. z o.o. określone w art. 39 RODO.

V. ODPOWIEDZIALNOŚĆ

1. Administrator Danych Osobowych

Administratorem Danych Osobowych jest osoba decydująca o celach i środkach przetwarzania danych osobowych, którą są Zakłady Mleczarskie Laktopol-A Sp. z o.o. W imieniu ADO stroną reprezentująca jest zgodnie z zapisami KRS. Administrator Danych Osobowych odpowiada za zapewnienie technicznych i organizacyjnych warunków dla bezpieczeństwa przetwarzanych danych osobowych odpowiednich do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności za bezpieczeństwo danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, utratą, uszkodzeniem, lub zniszczeniem.

Do zadań ADO należy:

1. Nadzór zachowania „szczególnej staranności" oraz przestrzeganie zasad:

1.1. Legalności przetwarzania danych osobowych będących w posiadaniu podmiotu,

1.2. Niezmieniania celu przetwarzania danych,

1.3. Merytorycznej poprawności danych oraz ich adekwatności w stosunku do celów, w jakim dane te są przetwarzane,

1.4. Czasowego przetwarzania danych (nie dłużej, niż jest to niezbędne do realizacji celu ich przetwarzania),

2. Administrator zobowiązany jest do informowania podmiotu, którego dane dotyczą – każdorazowo na wniosek zainteresowanego/ osoby fizycznej.
3. Powoływanie i odwoływanie w drodze zarządzeń Inspektora Ochrony Danych Osobowych oraz Administratora Systemu Informatycznego.
4. Podejmowania decyzji o zakupie, modernizacji, wymianie wszelkich rozwiązań technicznych i technologicznych zapewniających bezpieczne przetwarzania danych osobowych na wniosek IODO i ASI (odpowiednio do stopnia eksploatacji, poziomu gwarantowanego bezpieczeństwa, aktualnych rozwiązań technicznych).
5. Zatwierdzanie pod względem formalno – prawnym wszystkich dokumentów w ramach polityki bezpieczeństwa.

2. Inspektor Ochrony Danych Osobowych (IODO)

W związku z prawnym aspektem co do kryteriów konieczności wyznaczania Inspektora Ochrony Danych Osobowych – Art 37 RODO, decyzją Administratora Danych Osobowych, funkcja ta została powierzona w drodze Zarządzenia Prezesa. Szczegółowy zakres zadań odpowiedzialności i uprawnień Inspektora ochrony Danych Osobowych wyspecyfikowano w załączniku Nr 1 do uprzednio cytowanego zarządzenia.

3. Administrator Systemu Informatycznego (ASI)

Administrator Danych Osobowych w drodze decyzji powołał Administratora Systemu Informatycznego odpowiedzialnego za całokształt działań w ramach poprawności funkcjonowania i zapewnienia właściwego poziomu bezpieczeństwa systemu informatycznego.

Do zadań Administratora Systemu Informatycznego w zakresie ochrony danych osobowych w ramach powierzonej funkcji należy:

1. koordynacja wdrażania i monitorowanie działań w ramach wdrożonych zabezpieczeń technicznych i organizacyjnych, mających na celu ochronę przetwarzania danych osobowych w systemach informatycznych,
2. Przydzielanie praw dostępu do przetwarzania danych osobowych w systemie informatycznym dla pracowników i/ lub osób stale współpracujących z Zakładem, na podstawie indywidualnych upoważnień,
3. Monitorowanie i analiza stanu sprzętu i urządzeń technicznych przetwarzających dane osobowe, bieżąca ich modernizacja zgodnie z rozwojem techniki adekwatnie do rodzaju wykorzystywanego sprzętu,
4. Zabezpieczenie urządzeń, dysków lub innych nośników informatycznych, zawierających dane osobowe, przeznaczonych do likwidacji, tak by uprzednio były pozbawione zapisu tych danych, a w przypadku, gdy nie jest to możliwe - zostały uszkodzone w sposób uniemożliwiający ich odczytanie,
5. Zabezpieczenie urządzeń, dysków lub innych nośników informatycznych, zawierających dane osobowe, przeznaczonych do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania danych osobowych, tak aby były uprzednio pozbawione zapisu danych, a w przypadku, gdy nie jest to możliwe - zostały uszkodzone w sposób uniemożliwiający ich odczytanie,
6. Zabezpieczenie urządzeń, dysków lub innych nośników informatycznych, zawierających dane osobowe, przeznaczonych do naprawy, tak aby zostały uprzednio pozbawione zapisu tych danych, a gdy jest to niemożliwe - aby były naprawione pod nadzorem osoby upoważnionej,
7. Analiza informowanie kierowników jednostek organizacyjnych o przekroczeniu uprawnień, naruszeniu zasad bezpieczeństwa obowiązujących przy przetwarzaniu danych osobowych,
8. Prowadzenie szkoleń dla pracowników przetwarzających dane osobowe w systemie informatycznym,
9. Stała współpraca z Administratorem Danych Osobowych oraz Inspektorem Ochrony Danych Osobowych w zakresie bezpieczeństwa i ochrony danych osobowych,

W celu realizacji powierzonych zadań Administrator Systemu Informatycznego w zakresie ochrony danych osobowych ma prawo:

1. kontrolować komórki organizacyjne/ stanowiska Zakładu pod kątem właściwego zabezpieczenia danych osobowych w przetwarzanych w systemie informatycznym,

2. informować Właściciela/Administratora Danych Osobowych oraz Inspektora Ochrony Danych Osobowych w przypadkach naruszenia bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym,

Administrator Systemu Informatycznego w zakresie ochrony danych osobowych ma obowiązek sprawdzenia czy naruszenie zasad ochrony danych osobowych nastąpiło z winy pracownika i/ lub osoby stale współpracującej z Zakładem oraz zabezpieczenia materiałów niezbędnych do wyjaśnienia sprawy,

Jeżeli zachodzi podejrzenie, że naruszenie lub zagrożenie bezpieczeństwa ochrony danych osobowych jest wynikiem przestępstwa, Administrator Systemu Informatycznego w zakresie ochrony danych osobowych w porozumieniu z Właścicielem/Administratora Danych Osobowych oraz Inspektorem Ochrony Danych Osobowych zawiadamia o powyższych okolicznościach właściwe organy.

4. Kadra kierownicza na poziomie operacyjnym

Kadra kierownicza Zakładu stanowi niezwykle ważny obszar w strukturze organizacyjnej w aspekcie właściwego wdrożenia i funkcjonowania zasad ustanowionej polityki bezpieczeństwa i ochrony danych osobowych. Do zadań kadry kierowniczej w aspekcie poprawności i prawidłowości funkcjonowania przyjętej Polityki należy:

1. Bieżący nadzór i kontrolę przestrzegania zasad przyjętych w niniejszym dokumencie oraz dokumentacji systemu zarządzania jakością regulujące zasady postępowania w zakresie bezpieczeństwa informacji w tym ochrony danych osobowych,
2. Reagowanie na wszelkie nieprawidłowości w zakresie bezpieczeństwa informacji w tym ochrony danych osobowych w podległym im obszarze,
3. Zgłaszanie wszelkich informacji/ zdarzeń itp. związanych w bezpieczeństwem informacji i ochroną danych osobowych w odniesieniu do podległego im obszaru do Inspektora Ochrony Danych Osobowych opcjonalnie Dyrektora Zakładu,
4. Zgłaszanie pomysłów, wniosków racjonalizatorskich których celem będzie poprawa bezpieczeństwa informacji w tym ochrony danych osobowych.

5. Pracownicy/ osoby współpracujące

Pracownicy/ osoby współpracujące z Zakładami posiadający stosowane upoważnienia do przetwarzania danych osobowych oraz dostęp do zbiorów danych osobowych mają obowiązek przestrzegania postanowień dokumentu Polityki Bezpieczeństwa oraz szczegółowych procedur postępowania w tym również, przepisów prawa regulujących kwestie bezpieczeństwa i ochrony przetwarzanych danych osobowych. Użytkownik systemu informatycznego ma prawo do wykonywania tylko tych czynności, do których został upoważniony. Użytkownik systemu ponosi wszelką odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.

Wszelkie przekroczenia lub jakiekolwiek próby przekroczenia przyznanych uprawnień, traktowane będą, jako naruszenie podstawowych obowiązków pracowniczych lub naruszenie zapisów umowy. Każdy pracownik/ osoba współpracująca z Zakładem wykonująca zadania związane z przetwarzaniu danych osobowych zobowiązany jest do zachowania ich w poufności oraz dołożenia wszelkich starań, aby dane osobowe nie zostały przekazane osobom nieuprawnionym lub nie zostały użyte w sposób niezgodny z ich przeznaczeniem.

VI. ZASADY DOTYCZĄCE PRZETWARZANIA DANYCH OSOBOWYCH

Przetwarzanie danych osobowych jest zgodne z prawem krajowym/Unijnym wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:

a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów,
b) 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,
c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze,
d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej,
e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi,
f) 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.

Szczegółowe zasady przetwarzania danych osobowych regulują odpowiednie przepisy prawa. Administrator Danych Osobowych zobowiązany jest do bieżącego śledzenia aktualności wymagań prawnych (we współpracy z osobami odpowiedzialnymi za poszczególne obszary w Zakładzie w ramach których przetwarzane są dane osobowe) oraz terminowe informowanie Administratora i Inspektora Ochrony Danych Osobowych o pojawiających się zmianach i wynikających z nich potrzebach.

Każdorazowo o ile nie istnieją prawne przesłanki do przetwarzania danych osobowych jako warunek niezbędny/ konieczny do zrealizowania usługi lub w obszarze administracyjno – organizacyjnym Zakładu Administrator Danych Osobowych zobowiązany jest dopełnić należytych starań, aby uprzednio przed podjęciem realizacji usługi, pozyskać od osób fizycznych, których dane będę przetwarzane oświadczenie zgody. Szczegółowo kwestie związane z pozyskaniem i zabezpieczaniem dowodu zgody na przetwarzanie danych osobowych reguluje ***Procedura PO-4 – zasady przetwarzania/archiwizowania dokumentu wyrażonej zgody na przetwarzanie danych osobowych***.

VII. RODZAJE PRZETWARZANYCH DANYCH OSOBOWYCH

Zakłady Mleczarskie Laktopol-A Sp. z o.o. w zakresie prowadzonej działalności/prowadzonych działań operacyjnych przetwarzają dane osobowe:

a) Pracowników/ osób współpracujących z Zakładem,
b) Kontrahentów w ramach prowadzonej współpracy,

W większości przypadku prowadzonych działań operacyjnych Zakład przetwarza dane osobowe tzw. zwykłe typu imię i nazwisko, nr telefonu, adres e- mail. Jedynie w incydentalnych przypadkach przetwarzane są szczególne kategorie danych osobowych dotyczą pracowników Zakładu– w tzw. sytuacjach szczególnych tj. Wypadki przy pracy, zaświadczenia lekarskie itp. Administrator Danych Osobowych każdorazowo przed podjęciem nowych działań operacyjnych/ dotychczas nie realizowanych których specyfika związana jest z przetwarzaniem danych osobowych zobowiązany jest dokonać szczegółowej analizy kategorii osób których dane będą przetwarzane jak i zakresu

i rodzaju danych tak aby właściwie oszacować potencjalne ryzyko związane z niniejszymi operacjami i wdrożyć właściwe środki zaradcze gwarantujące odpowiedni poziom ochrony i bezpieczeństwa danych.

VIII. ORGANIZACJA DZIAŁAŃ W ZAKŁADZIE W RAMACH PRZETWARZANIA DANYCH OSOBOWYCH

Dane osobowe przetwarzane w ramach realizowanych procesów/ działań operacyjnych w Zakładach Mleczarskich Laktopol-A Sp. z o. o. dotyczą organizacji i zarządzania procesami handlowymi, sprzedażowymi i marketingowymi. Osobny rodzaj procesów związanych z przetwarzaniem danych osobowych stanowi obsługa kadrowa.

W przypadku konieczności pozyskania zgody od osób których dane osobowe będą przetwarzane Administrator Danych Osobowych decyduje o kształcie klauzuli zgody jak i o obowiązku informacyjnym ciążącym na nim w tej sytuacji. Niniejsze działania realizowane są zgodnie z Procedurą ***PO-4 – zasady przetwarzania/archiwizowania dokumentu wyrażonej zgody na przetwarzanie danych osobowych***.

IX. WARUNKI WYRAŻENIA ZGODY

Wszędzie tam gdzie specyfika realizowanych zadań operacyjnych wymaga pozyskiwanie i przetwarzania danych osobowych i niej spełnione są przesłanki do przetwarzania niniejszych danych na podstawie litery prawa, umowy czy prawnie uzasadnionego interesu Administratora pozyskiwana jest zgoda na przetwarzanie danych osobowych. 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. Zgoda powinna być wyrażona w drodze jednoznacznej, potwierdzającej czynności, która wyraża odnoszące się do określonej sytuacji dobrowolne, świadome i jednoznaczne przyzwolenie osoby, których dane dotyczą, na przetwarzanie dotyczących jej danych osobowych i która ma na przykład formę pisemnego (w tym elektronicznego) lub ustnego oświadczenia. Może to polegać na zaznaczeniu okienka wyboru podczas przeglądania strony internetowej, na wyborze ustawień technicznych do korzystania z usług społeczeństwa informacyjnego lub też na innym oświadczeniu bądź zachowaniu, które w danym kontekście jasno wskazuje, że osoba, której dane dotyczą, zaakceptowała proponowane przetwarzanie jej danych osobowych. Milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania nie powinny zatem oznaczać zgody. Zgoda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeżeli przetwarzanie służy różnym celom, potrzebna jest zgoda na wszystkie te cele. Jeżeli osoba, której dane dotyczą, ma wyrazić zgodę w odpowiedzi na elektroniczne zapytanie, zapytanie takie musi być jasne, zwięzłe i nie zakłócać niepotrzebnie korzystania z usługi, której dotyczy.

X. INFORMACJE PODAWANE W PRZYPADKU ZBIERANIA DANYCH OD OSOBY KTÓREJ DANE DOTYCZĄ

Administrator Danych Osobowych zobligowany jest do publikowania danych w ramach tzw. obowiązku informacyjnego wszędzie tam gdzie przetwarzanie odbywa się na podstawie wyrażonej zgody. Z chwilą wystandaryzowania wzoru klauzuli zgody Administrator Danych Osobowych określa treść obowiązku informacyjnego jak również podejmuje decyzję co do formy jego publikacji.

Podobnie jak wzór klauzuli zgody, treść obowiązku informacyjnego podlega okresowej weryfikacji i aktualizacji przez Inspektora Ochrony Danych Osobowych we współpracy z Administratorem Danych Osobowych. Niezależnie od powyższego dla zagwarantowania poprawności działania jak i rzetelności przetwarzania danych osobowych Administrator Danych Osobowych publikuje za pośrednictwem strony internetowej Zakładu w zakładce kontakt //

„dane osobowe" podstawowy zakres informacji w ramach procesu przetwarzania danych osobowych. Za nadzór i koordynację działań w ramach poprawności publikowanych informacji na stronie internetowej Zakładu odpowiada Inspektor Ochrony Danych Osobowych we współpracy z Administratorem Systemu Informatycznego.

XI. PRAWA OSÓB KTÓRYCH DANE SA PRZETWARZANE I ZASADY ICH RESPEKTOWANIA

Administrator Danych Osobowych zobowiązany jest zapewnić pełna możliwość respektowania praw osób których dane osobowe są przetwarzane w tym między innymi:

- Prawo dostępu przysługujące osobie, której dane dotyczą (uzyskiwania informacji) (Art. 15 RODO)
- Prawo do sprostowania danych (Art. 16 RODO)
- Prawo do usunięcia danych („prawo do bycia zapomnianym") – (Art. 17 RODO)
- Prawo do ograniczenia przetwarzania (Art. 18 RODO)
- Prawo do przenoszenia danych (Art. 20 RODO)
- Prawo sprzeciwu (Art. 21 RODO)

Każdorazowo w ramach zgłoszenia się do Zakładu osoby z żądaniem prawa w zakresie przetwarzanych danych dotyczących jego osoby, pracownik odbierający takowa informację zobowiązany jest:

- właściwie ją odnotować,
- niezwłocznie przekazać do ADO i/lub do Inspektora Ochrony Danych Osobowych.
- podjąć działania informacyjne, aktualizacyjne lub inne w zależności od żądania osoby wnioskującej.

W przypadku zaistnienia sytuacji, kiedy przepis innego aktu prawnego stanowi inaczej tj. zakłada dalej idącą ochronę lub wymóg archiwizacji, zastosowanie maja niniejsze przepisy prawa, co jednocześnie nie zwalnia ADO z obowiązku udzielenia stosownej informacji. Administrator Danych Osobowych zobowiązany jest do przedłożenia/przesłania osobie wnioskującej stosownej odpowiedzi. W sytuacji powierzania danych podmiotom przetwarzającym lub udostępniania danych innym administratorom danych należy ich powiadamiać o każdym sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych, które było wynikiem realizacji wniosku otrzymanego od osoby, której dane dotyczą. Osobą odpowiedziała za właściwe zredagowanie pisma, jak również archiwizację i nadzór w tym zakresie sprawuje Inspektor Ochrony Danych Osobowych.

XII. POWIERZANIE PRZETWARZANIA DANYCH OSOBOWYCH

Jeżeli przetwarzanie ma być dokonywane w imieniu Administratora Danych Osobowych, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi rozporządzenia ogólnego i chroniło prawa osób, których dane dotyczą. O wyborze podmiotu spełniającego wymagane kryteria poprawności i bezpieczeństwa przetwarzania decyduje Administrator Danych Osobowych. Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje Administratora Danych Osobowych o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian. Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania,

charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora. Ta umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający:

a) przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny,
b) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy,
c) podejmuje wszelkie środki gwarantujące należyty poziom bezpieczeństwa i ochrony przetwarzanych danych osobowych.

Szczegółowe zasady postępowania w ramach zawierania, archiwizacji i monitorowania poprawności realizacji zadań w ramach umowy powierzenia określa ***Procedura PO-5 – zasady powierzania przetwarzania danych osobowych.***

XIII. REJEST CZYNNOŚCI PRZETWARZANIA

Administrator Danych Osobowych zobowiązany jest odpowiednio do wymagań prawnych Rozporządzenia do prowadzenia rejestru czynności przetwarzania danych osobowych. Niniejszy rejestr sporządzany jest w oparciu o szczegółową inwentaryzację procesów/ działań operacyjnych i przetwarzanych w nich danych osobowych. Rejestr prowadzony jest w wersji elektronicznej, pod nadzorem Inspektora Ochrony Danych osobowych, podlega bieżącej aktualizacji każdorazowo o ile wystąpią jakiekolwiek zmiany w zakresie prowadzonych działań operacyjnych i przetwarzanych w nich danych osobowych.

Rejestr czynności przetwarzania udostępniany jest każdorazowo na żądanie organu nadzorczego. W innych sytuacjach decyzję co do udostepnienia rejestru operacji podejmuje Administrator Danych Osobowych. Z uwagi na istotność danych zawartych w rejestrze dla działalności Zakładu jak i ustanowionej Polityki jest on zabezpieczony przed nieautoryzowaną zmianą, modyfikacją itp.

XIV. ZGŁOSZENIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Incydent związany z bezpieczeństwem informacji - to pojedyncze zdarzenie lub seria zdarzeń niepożądanych albo niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji, w tym danych osobowych. Szczegółowo zasady postepowania w ramach wystąpienia incydentu naruszenia bezpieczeństwa i ochrony danych osobowych reguluje ***Procedura PO – 6 zasady postępowania w przypadku incydentu naruszenia bezpieczeństwa przetwarzania danych osobowych.***

XV. DOBÓR ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH DOTYCZĄCYCH PRZETWARZANIA I ZABEZPIECZANIA DANYCH OSOBOWYCH

Dobór środków technicznych i organizacyjnych dotyczących przetwarzania i zabezpieczania danych osobowych w Zakładzie realizowany jest w oparciu o szacowanie ryzyka naruszenia praw i wolności osób, których dane

dotyczą. Zasady dotyczące przeprowadzania szacowania ryzyka naruszenia praw i wolności osoby fizycznej określone zostały w Rozdziale XVI niniejszej Polityki. Przy doborze zabezpieczeń należy i oceniać ryzyko zarówno w kontekście skutków dla osoby, której dane dotyczą w tym np. dyskryminacja, pozbawienie przysługujących praw, szkody majątkowe i niemajątkowe), jak również ryzyko w kontekście skutków dla Zakładu w przypadku niepodjęcia działań związanych zapewnienie przetwarzania danych osobowych zgodnie z RODO. Dobór zabezpieczeń dla systemów informatycznych wykorzystywanych do przetwarzania danych następuje na podstawie procedur szacowania ryzyka przyjętych w Zakładzie w tym również rekomendacji Administratora Systemu Informatycznego zakresie możliwych do zastosowania rozwiązań technicznych. Ustalone wymagania dotyczące zabezpieczenia danych osobowych w odniesieniu do danego procesu przetwarzania danych osobowych są odnotowywane przez Inspektora Ochrony Danych w prowadzonym rejestrze czynności przetwarzania danych osobowych. Planowanie realizacji nowych procesów związanych z przetwarzaniem danych osobowych, w tym w szczególności nowych systemów informatycznych służących do przetwarzania danych osobowych, musi uwzględniać zasady ochrony danych w fazie projektowania („privacy by design") oraz domyślnej ochrony danych („privacy by default").

Projektowanie nowych usług związanych z przetwarzaniem danych osobowych wspieranych przez systemy informatyczne odbywa się w ramach bieżących działań operacyjnych prowadzonych przez Właściciela we współpracy z pracownikami operacyjnymi oraz Administratorem Systemu Informatycznego. W przypadku realizacji procesów przetwarzania danych osobowych w Zakładzie, które ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, przed rozpoczęciem przetwarzania należy dokonać oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych zgodnie z art. 35 RODO. Jeżeli dokonana ocena skutków dla ochrony danych wykaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby nie zostały zastosowane środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania należy skonsultować się z krajowym organem nadzoru ochrony danych osobowych. W przypadku konieczności przeprowadzenia konsultacji z organem nadzorczym Inspektor Ochrony Danych Osobowych przygotowuje odpowiedni wniosek o konsultacje zgodnie z art. 36 RODO i kontaktuje się w tej sprawie z organem.

XVI. ANALIZA RYZYKA DLA OPERACJI NA DNAYCH OSOBOWYCH

Każdy z pracowników odpowiedzialnych za poszczególne obszary operacyjne Zakładu zobowiązany jest raz w roku w ustalonym przez Inspektora Ochrony Danych Osobowych terminie dokonać analizy sytuacji/stanu realizowanego procesu w aspekcie przetwarzanych danych osobowych a w tym:

a. ocenić zdolność procesu do realizacji zamierzonego celu w aspekcie właściwego postępowania z przetwarzanymi danymi osobowymi w tym możliwości zachowania ich należytego poziomu bezpieczeństwa,
b. poprzez prezentację wyników monitorowania procesu za ostatnie 12 miesięcy, w tym działania korygujące, które zostały podjęte w ciągu roku po zaistniałych incydentach dotyczących przetwarzanych danych osobowych,
c. dokonać szczegółowej analizy rodzaju/zbioru przetwarzanych danych osobowych w ramach procesu w szczególności nowych zadań/ obszarów/ aktywności w ramach których przetwarzane są dane osobowe dotychczas nieidentyfikowane.

Uzyskane dane stanowią wstępny zakres działań w ramach analizy i oceny ryzyka i zagrożeń dla aktywów informacyjnych w tym przetwarzanych danych osobowych w poszczególnych obszarach.

Metodyka analizy i oceny ryzyka

Etap I Przygotowanie

1. W ramach analizy procesu należy uwzględnić czynniki istotne dla realizacji zadań i przebiegu procesu mające związek z zapewnieniem właściwego poziomu bezpieczeństwa przetwarzanych danych w tym dotyczące bezpieczeństwa przetwarzanych danych osobowych w procesie tj.
2. Analizę kontekstu przeprowadzamy w trzech aspektach:
   a. aspekt finansowy
   b. aspekt prawny
   c. aspekt organizacyjny (ludzie, infrastruktura, zasady, wartości, kultura organizacji itp.)
3. Identyfikujemy wymagania i wpływa stron zainteresowanych mających wpływ na realizację zadań/procesu jak i zakres/bezpieczeństwo przetwarzanych danych w tym danych osobowych.
4. Każdy z elementów kontekstu jak i stronę zainteresowaną należy poddać odpowiedniej kwantyfikacji w zakresie mocnych stron, słabych stron oraz szans i zagrożeń.
5. Działania związane z przeprowadzeniem analizy i oceny ryzyka dla aktywów informacyjnych w tym przetwarzanych danych osobowych powinna być prowadzona przez Właściciela procesu = osobę odpowiedzialną za dany obszar w Zakładzie, z udziałem kluczowych pracowników bezpośrednio zaangażowanych w realizację zadań w ramach procesu i przetwarzanie danych osobowych, wskazany udział Specjalisty ds. IT.
6. Wymagane jest zarezerwowanie odpowiedniej ilości czasu/warunków aby proces analizy i oceny ryzyka przeprowadzony został z należytą starannością
7. Zespół dokonuje szczegółowej identyfikacji aktywów informacyjnych w tym danych osobowych przetwarzanych w ramach procesu.
8. Zidentyfikowane aktywa wpisujemy do arkusza RA procesu _ kolumna „C" – „Nazwa aktywa/grupy aktywów/przetwarzanych danych osobowych"
9. Jeżeli dane aktywo jest daną osobową – w kolejnym etapie należy określić rodzaj operacji związanych z przetwarzaniem danych osobowych.
10. Identyfikujemy właściciela zasobu oraz formę przetwarzania aktywów/ danych osobowych.

Etap II Identyfikacja zagrożeń

1. Dla zidentyfikowanych procesów i przetwarzanych w nich aktywów informacyjnych/danych osobowych lub grupy/zbiorów aktywów, danych identyfikujemy zagrożenia mogące mieć związek z realizacją zadań w procesie w tym z przetwarzaniem danych osobowych.
2. Zagrożenie definiuje się jako potencjalną negatywną sytuację/zdarzenie mające wpływ na cel w procesie tym samym negatywnie skutkujące dla bezpieczeństwa przetwarzanych danych osobowych.
3. Identyfikując zagrożenia (najbardziej prawdopodobne/realne co do wystąpienia) korzystamy ze zdefiniowanej listy tj.
   - trwałe zniszczenie zbiorów papierowych
   - dekompletacja zbiorów papierowych
   - kradzież zbiorów papierowych
   - zgubienie / usunięcie do kosza zbiorów papierowych
   - uszkodzenie (np. wyblaknięcie, zalanie) zbiorów papierowych

- nieumyślne przekazanie osobom nieuprawnionym zbiorów papierowych
- dostęp nieuprawnionych osób do pomieszczenia ze zbiorami papierowymi
- zbyt długie przechowywanie
- zbyt krótkie przechowywanie
- skasowanie danych zbiorów elektronicznych
- wyciek danych (włamanie)
- uszkodzenie nośnika dla zbiorów elektronicznych
- błąd w modyfikacji zbiorów elektronicznych (np. nadpisanie wersji)
- brak dostępu (czasowy lub stały) do zbiorów elektronicznych
- dostęp osób nieuprawnionych do zbiorów elektronicznych
- brak kopii zapasowych dla zbiorów elektronicznych
- złośliwe działanie człowieka wobec zbiorów elektronicznych

4. W kolumnie „H" szczegółowo opisujemy zagrożenie, które może wystąpić.
5. Jeżeli dane aktywo informacyjne – jest daną osobową – należy dokonać oceny wartości przetwarzanych danych korzystając ze zdefiniowanej skali oceny jakościowej tj.
   a. 1- bardzo niska - dane osobowe zwykłe, przetwarzane incydentalnie, ich utrata/nie wyrządzi szkód fizycznych, majątkowych lub niemajątkowych dla osoby fizycznej (mogą być powszechnie dostępne w przestrzeni publicznej)
   b. 2- niska - dane osobowe zwykłe, przetwarzane na podstawie prawa lub udzielonej zgody, występujące w postaci kopii dokumentów/ danych, ich utrata/nie wyrządzi szkody fizycznej, szkód majątkowych lub niemajątkowych dla osoby fizycznej
   c. 3- średnia - dane osobowe zwykłe lub szczególne przetwarzane na podstawie prawa lub udzielonej zgody, występujące w postaci kopii dokumentów/ danych wymagające prawnej ochrony i zabezpieczeń, utarta może wyrządzić szkodę majątkową lub niemajątkową dla osoby fizycznej,
   d. 4- wysoka - dane osobowe zwykłe, przetwarzane na podstawie prawa lub udzielonej zgody, incydentalnie, wymagające prawnej ochrony i zabezpieczeń, wymagające prawnej ochrony i zabezpieczeń, ich utarta może wyrządzić szkodę majątkową lub niemajątkową dla osoby fizycznej.
6. W dalszym etapie identyfikujemy:
   6.1. lokalizację / miejsce/ miejsce/ dział Firmy gdzie zarażenie może wystąpić,
   6.2. Aktualne zabezpieczenia tj. rozwiązania organizacyjne, proceduralne, systemowe, fizyczne pozwalające zapobiegać wystąpieniu zagrożenia.
   6.3. Aspekt bezpieczeństwa tj poufność, integralność, dostępność jaki będzie miał miejsce w sytuacji zaistnienia zagrożenia.

Etap III Analiza ryzyka

1. Dla zidentyfikowanych aktywów informacyjnych w tym przetwarzanych danych osobowych lub grupy aktywów /zbiorów danych i przypisanych im zagrożeń Zespół ocenia **podatności** tj. słabości danych/zbioru danych/ procesu mogąca być wykorzystana przez zagrożenie i spowodować jego urealnienie.

2. W odniesieniu do zidentyfikowanych zagrożeń jak i obecnych zabezpieczeń należy określić **prawdopodobieństwo** wystąpienia danego zagrożenia korzystając ze zdefiniowanej skali:

1- mało prawdopodobne, raczej się nie zdarzy

2- prawdopodobieństwo małe, istnieje szansa wystąpienia, ale z naszego doświadczenia wiemy że rzadko występuje

3- prawdopodobieństwo średnie - istniej możliwość wystąpienia zagrożenia

4- prawdopodobieństwo wysokie istnie bardzo realna szansa na wystąpienie zagrożenia

5- prawdopodobieństwo bardzo wysokie wiemy to z doświadczenia miało już miejsce w organizacji.

3. Następnie identyfikujemy **skutek** – potencjalną dotkliwość dla procesu i przetwarzanych w nim aktywów informacyjnych w tym danych osobowych. Korzystając ze zdefiniowanej skali:

A- pomijalny, wystąpienie zagrożenia w żaden sposób nie zaburzy działań w procesie, ani wpłynie na przetwarzane aktywa informacyjne/ dane osobowe,

B- mały, wystąpienie zagrożenia może spowodować zakłócenia w pracy przy czym nie wpłyną one na przerwanie ciągłości działania,

C- średni, wystąpienie zagrożenia może spowodować zakłócenia w pracy, zaburzona zostanie ciągłość działania zadań w procesie, zagrożona jest realizacja celu procesu,

D- znaczący, wystąpienie zagrożenia, spowoduje zakłócenia w pracy, zaburzona zostanie ciągłość działania zadań w procesie, zagrożona jest realizacja celu procesu,

E- katastrofalny , wystąpienie zagrożenia spowoduje znaczące przerwy w pracy, ciągłość działania procesu zostaje poważnie zaburzona, cel procesu nie zostanie osiągnięty, dojdzie do szkody i strat.

4. Kolejnym etapem jest zdefiniowanie poziomu ryzyka w oparciu o wynik dla prawdopodobieństwa i skutku (korzystając z wzoru matrycowego)

			SKUTEK				
			Bardzo niski	Niski	Średni	Wysoki	Bardzo wysoki
			A	B	C	D	E
PRAWDOPODOBIEŃSTWO	Prawie pewne	5	Ś	W	K	K	K
	Prawdopodobne	4	Ś	W	W	K	K
	Możliwe	3	N	Ś	W	W	K
	Mało prawdopodobne	2	N	Ś	Ś	W	W
	Rzadkie	1	N	N	Ś	Ś	W

5. Po zdefiniowaniu poziomu ryzyka dla zidentyfikowanych aktywów informacyjnych i danych osobowych lub grupy/zbiorów danych w procesie należy dokonać oceny skutków dla Zakładu w aspekcie skuteczności funkcjonowania zasad bezpieczeństwa, opcjonalnie w przypadku danych osobowych dla ADO jak i osoby fizycznej.
6. Odpowiednio do zidentyfikowanego poziomu ryzyka i skutków dla osoby fizycznej której dane dotyczą Zespół określa czynniki okoliczności jakie wpłynęły na wynik oceny ryzyka = uzasadnienie do oceny.

IV – Decyzja co do podjęcia działań w ramach zidentyfikowanego poziomu ryzyka

1. Zespół poddaje szczegółowej analizie pozom zdefiniowanego ryzyka, jego istotność w aspekcie skutku dla: ADO/osoby fizycznej której dane dotyczą, wpływu na cele w procesie, zdefiniowane priorytety, możliwości, plany rozwojowe itp. i na tej podstawie Właściciel Procesu podejmuje decyzje co do dalszych sposobu postępowania ze zidentyfikowanym ryzykiem
2. Proponowane sposoby postepowania: akceptacja, akceptacja_ monitoring i kontrola, działania doskonalące/wdrożenie zabezpieczeń, transfer ryzyka, podjęcie ryzyka.
3. Ocena skutków oszacowanego ryzyka prowadzona jest w aspekcie Administratora Danych Osobowych jak i osoby fizycznej której dane dotyczą.

Poziom ryzyka	Opis działania
Niski (N)	Poziom ryzyka akceptowany – działania podejmowane w zależności od wymaganych nakładów
Średni (Ś)	Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, ale wymaga okresowego monitorowania
Wysoki (W)	Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, ale wymaga stałego monitorowania
Krytyczny (K)	Poziom ryzyka nietolerowany – wymaga natychmiastowego działania

IV – Wskazanie działań doskonalących /wdrożenie zabezpieczeń jakie należy podjąć

1. W przypadku podjęcia decyzji o działaniach doskonalących/wdrożeniu zabezpieczeń mających na celu wyeliminowania ryzyka lub jego zminimalizowanie do poziomu akceptowalnego Właściciel procesu określa rodzaj działań lub wpisuje informację o planowanych działaniach.
7. Działania zaplanowane do wdrożenia dla zidentyfikowanych danych osobowych lub grupy/zbiorów danych w procesie i zdefiniowanego ryzyka szczegółowo dokumentowane są w Planie postepowaniu z ryzykiem w arkusza RA procesu_ w zakładce „Szacowanie ryzyka i plan” – część „Plan postepowaniu a ryzykiem”

V. Ocena skuteczności

1. Każdorazowo przy kolejnej analizie i oceni ryzyka Właściciel Procesu/ osoba odpowiedzialna za dany obszar w Zakładzie, wszędzie tam gdzie podjęto działania doskonalące/ wdrożono zabezpieczenia powinien dokonać oceny ich skuteczność.

XVII. SZCZEGÓŁOWE PROCEDURY/ POLITYKI POSTEPOWANIA W RAMACH BEZPIECZEŃSTWA I OCHRONY DANYCH OSOBOWYCH

1. Procedura PO-1 – zasady nadawania, monitorowania i odbierania upoważnień do przetwarzania danych osobowych.
2. Procedura PO-2 – zasady przydzielania uprawnień w systemie informatycznym.
3. Procedura PO-3 – podstawowe zasady bezpieczeństwa informacji.
4. Procedura PO-4 – zasady przetwarzania danych osobowych na podstawie zgody.
5. Procedura PO-5 – zasady postepowania w przypadku powierzania przetwarzania danych osobowych.

6. Procedura PO-6- zasady postępowania w przypadku naruszenia bezpieczeństwa przetwarzanych danych osobowych.
7. Procedura PO-7 – zasady postępowania z wizytówkami i materiałami reklamowymi zawierającymi dane osobowe.
8. Procedura PO- 8 – zasady bezpiecznego przetwarzania danych osobowych.
9. Procedura PO -9 – zasady korzystania z elektronicznej służbowej skrzynki e-mail.
10. Regulamin funkcjonowania systemu informatycznego