POLITYKA BEZPIECZEŃSTWA

MERCATOR PAWEŁ ROKICKI 96-315 WISKITKI STARY DRZEWICZ 3

Data i miejsce sporządzenia dokumentu:	Wiskitki 25/05/2018
Ilość stron:	39

SPIS TREŚCI

1. WSTĘP

1.1. INFORMACJE OGÓLNE

1. Wskazanie Administratora Danych, który wdraża Politykę Bezpieczeństwa.

   Mercator Paweł Rokicki 96-315 Wiskitki Stary Drzewicz 3

2. Wyjaśnienie celu wprowadzania dokumentu.

   Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnego przepływu takich danych

3. Wskazanie podstaw prawnych.

   Dokument Polityki Bezpieczeństwa został opracowany w oparciu o wytyczne zawarte w następujących aktach prawnych:

   1)Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024 ze zm.),

   2)Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych.

   3)Ustawa o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000) z dnia 10 maja 2018 r.

1.2. ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ BEZPIECZEŃSTWA ORAZ ZAKRES ZASTOSOWANIA

1. Dokument Polityki Bezpieczeństwa opisuje zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem.

2. W powyższym podrozdziale wskazano zakres przedmiotowy Polityki Bezpieczeństwa wraz z elementami wymaganymi przepisami prawa.

Obligatoryjne elementy Polityki Bezpieczeństwa

Na Politykę Bezpieczeństwa składają się następujące informacje:

1) wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe:

- siedziba firmy Mercator Paweł Rokicki 96-315 Wiskitki Stary Drzewicz 3, pomieszczenie zajmowane przez Prezesa Firmy, pomieszczenie zajmowane przez pracowników firmy - stanowiska pracy
- biuro rachunkowe Biuro Rachunkowe "Cedar" Cebulscy spółka jawna ul. Jaśminowa 7 96-300 Korytów adres biura: ul. 1-go Maja 17 lok. 14 96-300 Żyrardów pomieszczenie biurowe- na II piętrze budynku

2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych:

- dane osobowe pracowników firmy Mercator Paweł Rokicki
- dane osobowe współpracowników firmy Mercator Paweł Rokicki
- dane osobowe klientów firmy Mercator Paweł Rokicki

3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,

Nazwa zbioru danych osobowych: Dane osób zatrudnionych

Cel przetwarzania: Realizacja obowiązków związanych ze stosunkiem pracy pracowników

Nazwa systemu, ewidencji lub aplikacji, w której przetwarzane są dane osobowe: akta osobowe

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi – akta, rejestry wykorzystywane w procesach kadrowo – płacowych wynikających ze stosunku pracy

Nazwa zbioru danych osobowych: Dane osób współpracujących

Cel przetwarzania: Realizacja obowiązków związanych z zawarciem umów cywilnoprawnych

Nazwa systemu, ewidencji lub aplikacji, w której przetwarzane są dane osobowe: rejestry zawierające umowy cywilnoprawne

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi – rejestry wykorzystywane w procesach kadrowo – płacowych wynikających z zakresu nawiązania i rozliczania umów cywilnoprawnych

Nazwa zbioru danych osobowych: Dane osobowe klientów firmy Mercator Paweł Rokicki

Cel przetwarzania: Realizacja zamówień, prowadzenie sprawozdawczości finansowej oraz marketing własnych produktów

Nazwa systemu, ewidencji lub aplikacji, w której przetwarzane są dane osobowe: zabezpieczone konta mailowe pracowników na serwerze obsługującym pocztę firmową, pliki tekstowe z tworzonymi umowami zapisane na dyskach twardych komputerów upoważnionych pracowników, kartoteka z umowami w wersji papierowej, program WF Mag, program Synergius.

4) Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania

między nimi – Dane osobowe pracowników i współpracowników: programy, rejestry wykorzystywane w procesach kadrowo – płacowych wynikających ze stosunku pracy

Dane osobowe klientów: imię i nazwisko , miejsce zatrudnienia, adres poczty elektronicznej, numer telefonu,

5) sposób przepływu danych pomiędzy poszczególnymi systemami,

Dane osób zatrudnionych - dane z kadrowej dokumentacji papierowej wprowadzane do programu kadrowego i Płatnik przez zewnętrzne biuro rachunkowe.

Dane osobowe współpracowników - dane z kadrowej dokumentacji papierowej wprowadzane do programu kadrowego i Płatnik przez zewnętrzne biuro rachunkowe.

Dane osobowe klientów: dane zapisane są w dokumentach w formie elektronicznej w programach WF Mag oraz Synergius

6) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Osoby przetwarzające dane posiadają imienne upoważnienia od Administratora Danych Osobowych, dokumentacja papierowa przechowywana w miejscu chronionym, systemy informatyczne zabezpieczone indywidualnymi hasłami uniemożliwiającymi dostęp osobom postronnym, z podmiotem przetwarzający dane osobowe zawarta umowa o powierzeniu danych osobowych.

1.3. WYJAŚNIENIE TERMINÓW UŻYWANYCH W DOKUMENCIE POLITYKI BEZPIECZEŃSTWA

2. Polityka Bezpieczeństwa posługuje się wieloma specjalistycznymi terminami z zakresu ochrony danych osobowych, które mogą być niewłaściwie rozumiane przez pracowników Administratora Danych – osoby obowiązane do przetwarzanie danych osobowych zgodnie z wymogami ustawowymi.

3. W powyższym podrozdziale wyjaśnia się znaczenie terminów i pojęć, które zawarte są w niniejszym dokumencie.

Przez użyte w Polityce bezpieczeństwa określenia należy rozumieć:

1. **Administrator danych osobowych –** osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych,

2. **Inspektor ochrony danych –** osoba wyznaczona przez administratora danych osobowych, nadzorująca przestrzeganie zasad i wymogów ochrony danych osobowych określonych w RODO i przepisach krajowych,
3. **ustawa –** Ustawa o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000) z dnia 10 maja 2018 r.
4. **RODO –** rozporządzenie Parlamentu Europejskiego i Rady /UE/ 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE /Dz. Urz. UE.L nr 119, str. 1/,
5. **dane osobowe –** wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej,
6. **zbiór danych osobowych –** uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów,
7. **przetwarzane danych –** operacja lub zestaw operacji wykonywanych na danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, łączenie, przesyłanie, zmienianie, udostępnianie i usuwanie, niszczenie, itd.,
8. **system informatyczny –** zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych,
9. **system tradycyjny –** zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji oraz wyposażenie i środki trwałe wykorzystywane w celu przetwarzania danych osobowych na papierze,
10. **zabezpieczenie danych w systemie informatycznym –** wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
11. **administrator systemu informatycznego –** osoba lub osoby, upoważnione przez administratora danych osobowych do administrowania i zarządzania systemami informatycznymi,
12. **odbiorca –** osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe w oparciu m. in. o umowę powierzenia,
13. **strona trzecia –** osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, które z upoważnienia administratora danych osobowych mogą przetwarzać dane osobowe,
14. **identyfikator użytkownika (login) –** ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
15. **hasło –** ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika,

znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

16. **poufność danych** – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.

2. OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

2.1. INFORMACJE OGÓLNE

1. Punkt ten wskazuje osoby odpowiedzialne za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami Ustawy, Rozporządzenia, Polityki Bezpieczeństwa oraz Instrukcji.

Katalog osób zajmujących określone stanowisko (pełniących określone funkcje) i zarazem odpowiadających za powyższe czynności jest niezmienny:

1. Administrator Danych Osobowych,
2. Inspektor Ochrony Danych Osobowych,
3. Osoby wykonujące pracę bądź świadczące usługi cywilnoprawne na rzecz Administratora Danych Osobowych, które uzyskały upoważnienie do przetwarzania danych osobowych,
4. Osoby, z którymi podpisano umowy powierzenia przetwarzania danych osobowych.

2.2. ADMINISTRATOR DANYCH

1. Administratorem Danych Osobowych jest Mercator Paweł Rokicki 96-315 Wiskitki Stary Drzewicz 3, NIP 8381624723.

1.1. Do ustawowych obowiązków Administratora należy:

1.1.1. Zapewnienie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:

- sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie dokumentacji;
- nadzorowanie opracowania i aktualizowania dokumentacji, oraz przestrzegania zasad w niej określonych;
- zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;

1.1.2 Administrator swoje ustawowe zadania może realizować, w szczególności poprzez:

- stały nadzór nad treścią Polityki Bezpieczeństwa i Instrukcji zarządzania systemem informatycznym,
- aktualizację i modyfikację ww. dokumentów,

- udział w kontrolach prowadzonych przez pracowników Urzędu Ochrony Danych Osobowych,
- udzielanie odpowiedzi na zapytania kierowane do Administratora Danych przez podmioty zewnętrzne, dotyczące administrowanych zbiorów danych osobowych,
- nadawanie poszczególnym pracownikom upoważnień do przetwarzania danych osobowych oraz przeprowadzanie dla nich szkoleń z zakresu ochrony danych osobowych
- nadzór nad nadawaniem uprawnień do przetwarzania danych osobowych w systemach informatycznych,
- prowadzenie aktualnej ewidencji osób upoważnionych do przetwarzania danych osobowych we wszystkich zbiorach oraz nadzór nad prowadzeniem rejestru nadanych uprawnień do przetwarzania danych w systemach informatycznych,
- nadzór nad fizycznym zabezpieczeniem obszarów, w których przetwarzane są dane osobowe,
- monitorowanie działania i skuteczności zabezpieczeń wdrożonych w celu ochrony danych osobowych.
- nadawanie / nadzór nad nadawaniem uprawnień do przetwarzania danych osobowych w systemach informatycznych,
- nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów,
- podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń,
- identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych i tradycyjnych,
- sprawowanie nadzoru nad przechowywanymi kopiami zapasowymi opisanymi w Instrukcji zarządzania systemem informatycznym.

1.1.3 Podstawowym obowiązkiem Administratora Danych Osobowych jest dbanie o to, aby przetwarzanie odbywało się zgodnie z rozporządzeniem RODO W tym celu, Administrator Danych Osobowych wdraża odpowiednie i skuteczne środki techniczne i organizacyjne:

- mają one zapewniać najwyższy, znany i możliwy w chwili przetwarzania danych, poziom ochrony;
- nie jest to czynność jednorazowa, środki te są w razie potrzeby poddawane przeglądom i uaktualniane;
- ochrony danych dokonuje się, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia;

- jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki te obejmują, wdrożenie przez Administrator Danych Osobowych, odpowiednich polityk ochrony danych;
- prowadzi komunikację z podmiotem danych i przekazuje mu informacje w sposób zwięzły, przejrzysty, zrozumiały i łatwo dostępny,
- ułatwia podmiotom danych wykonywanie ich praw,
- nieodpłatnie udziela podmiotom danych informacji, również na ich żądanie; czas na udzielenie informacji przez Administrator Danych Osobowych to maksymalnie miesiąc,
- weryfikuje tożsamość osób wnoszących żądania udzielenia informacji.
- potwierdza czy przetwarzane są dane osobowe dotyczące danej osoby fizycznej, a jeżeli ma to miejsce, udziela wskazanych rozporządzeniem informacji;
- ułatwia osobie, której dane dotyczą wykonywanie jej praw z art. 15–22 RODO;
- informuje osobę, której dane dotyczą, o działaniach jakie podjął, w związku z jej żądaniami opartymi o art. 15-22 RODO;
- uzasadnienia odrzucenie żądania osoby, której dane dotyczą i poucza ją o prawie skargi;
- umożliwia dostęp do jej danych osobie, której one dotyczą;
- dokonuje sprostowania i uzupełniania danych;
- usuwa dane;
- ogranicza przetwarzanie danych;
- powiadamia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu ich przetwarzania;
- dokonuje przenoszenia danych.

2. Inspektor Ochrony Danych Osobowych – w chwili obecnej ze względu na strukturę zatrudnienia oraz zakres przetwarzania danych osobowych nie powołuje się Inspektora Ochrony Danych Osobowych.
3. Osoby wykonujące pracę bądź świadczące usługi cywilnoprawne na rzecz Administratora Danych Osobowych, które uzyskały upoważnienie do przetwarzania danych osobowych,

   Osoba upoważniona obowiązana jest przetwarzać dane osobowe zawarte w ww. zbiorach danych osobowych w zakresie i w sposób wymagany do wypełnienia obowiązków służbowych względem Administratora Danych. Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem

4. Osoby, z którymi podpisano umowy powierzenia przetwarzania danych osobowych.

   Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 r. dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.

Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.

Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.

2.3.OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Każda osoba, która uzyskała upoważnienie do przetwarzania danych osobowych zobowiązana jest do ich ochrony w sposób zgodny z przepisami Ustawy, Rozporządzenia, Polityki Bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym.

2. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia.

3. UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. W punkcie tym opisano zasady nadawania upoważnień do przetwarzania danych osobowych osobom, które w ramach swoich obowiązków służbowych przetwarzają dane osobowe Administratora Danych.

Procedura nadawania upoważnień do przetwarzania danych osobowych powinna obejmować następujące informacje:

- Upoważnienie nadawane jest przez Administratora Danych Osobowych.
- Forma upoważnienia – pisemna.
- Forma zapoznania osoby upoważnionej z zasadami ochrony danych osobowych – po nadaniu upoważnienia i zapoznaniu pracownika z dokumentacją, procedurami, regulaminami pracownik podpisuje oświadczenie potwierdzające fakt zapoznania się z dokumentem. Podpisany dokument przechowywany jest w aktach osobowych pracownika
- Decyzję o nadaniu upoważnienia podejmuje Administrator, który ponosi odpowiedzialność za nadanie upoważnienia.
- Ewidencję nadanych upoważnień prowadzi Administrator.
- Forma prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych – forma papierowa.
- Wzór upoważnienia stanowi załącznik do Polityki Bezpieczeństwa.
- Wzór ewidencji osób upoważnionych do przetwarzania danych stanowi załącznik do Polityki Bezpieczeństwa.

4. UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych przewiduje możliwość powierzenie przetwarzania danych osobowych przez Administratora Danych zewnętrznym podmiotom.

1. Warunki zawierania umów powierzenia: powierzenie przetwarzania danych osobowych przez Administratora Danych zewnętrznym podmiotom może się odbywać wyłącznie na drodze umowy powierzenia, w której należy określić zbiór, który zostanie przekazany, cel tego przekazania oraz zakres planowanego przetwarzania danych przez inny podmiot.

2. Osoby odpowiedzialne za zgłoszenia Administratorowi Danych potrzeby zawarcia umowy powierzenia: pracownicy i współpracownicy firmy

3. Osoba odpowiedzialna za rejestrowanie zawartych umów powierzenia – Administrator Danych Osobowych.

5. OGÓLNE ZASADY BEZPIECZEŃSTWA OBOWIĄZUJĄCE PRZY PRZETWARZANIU DANYCH OSOBOWYCH

1. Wprowadzenie odpowiednich ze względu na charakter organizacji pracy Administratora Danych ogólnych zasad bezpieczeństwa przetwarzania danych - zgodnie z wymaganiami przepisów prawnych z zakresu ochrony danych osobowych – pozwoli na prawidłowe przetwarzanie danych.
2. Wskazano wykaz osób odpowiedzialnych za bezpieczeństwo przetwarzania danych – dotyczy to co do zasady wszystkich pracowników pracujących ze zbiorami danych.

- Za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze, indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik mający dostęp do danych.
- Pracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.
- W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. „czystego biurka”. Zasada ta oznacza nie pozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każdy z pracowników.
- Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe musi odbywać się w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek.
- Niedopuszczalne jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony.
- Przebywanie osób nieuprawnionych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych, chyba że dane te są w odpowiedni sposób zabezpieczone przed dostępem.
- Pracownicy zobowiązani są do zamykania na klucz wszelkich pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe w czasie ich chwilowej nieobecności w pomieszczeniu pracy, jak i po jej zakończeniu, a klucze nie mogą być pozostawione w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia posiadanych kluczy przed nieuprawnionym dostępem.

6. INSTRUKCJA POSTĘPOWNIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Procedura postępowania przypadku stwierdzenia naruszenia ochrony danych osobowych pozwalają na wypracowanie generalnych reguł dotyczących zachowania się pracowników Administratora Danych w przypadku wystąpienia naruszenia zasad ochrony danych osobowych.

2. Administrator Danych zobowiązany jest do stworzenia pewnego ogólnego trybu postępowania w wyżej wskazanej sytuacji, który będzie odpowiadać bądź organizacji pracy pracowników lub też specjalizacji prowadzonej działalności.

- Każda osoba, która poweźmie wiadomość w zakresie naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe bądź posiada informacje mogące mieć wpływ na bezpieczeństwo danych osobowych, jest zobowiązana fakt ten niezwłocznie zgłosić Administratorowi
- Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora osoba powiadamiająca powinna:
  - niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków, a następnie ustalić przyczyny, lub sprawców zaistniałego zdarzenia, jeżeli jest to możliwe,
  - zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,
  - udokumentować wstępnie zaistniałe naruszenie,
  - nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia.
- Po przybyciu na miejsce naruszenia ochrony danych osobowych, Administrator:
  - zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metod dalszego postępowania
  - wysłuchuje relacji osoby zgłaszającej z zaistniałego naruszenia, jak również relacji każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
- Administrator dokumentuje zaistniały przypadek naruszenia oraz sporządza raport.
- Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu, Administrator zasięga niezbędnych opinii i proponuje postępowanie naprawcze (w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń) i zarządza termin wznowienia przetwarzania danych.

- **Zgłaszanie naruszeń**

- w przypadku naruszenia ochrony danych osobowych w organizacji , administrator danych bez zbędnej zwłoki , w terminie 72 godzin po stwierdzeniu naruszenia, jest zobowiązany zgłosić takie naruszenie organowi nadzorczemu tj. PUODO, chyba, że jest mało prawdopodobne, by takie naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Naruszeniem praw lub wolności osób fizycznych zgodnie z RODO będzie m.in. powstanie uszczerbku fizycznego, szkód majątkowych lub niemajątkowych u osób fizycznych, takich jak: utrata kontroli nad własnymi danymi osobowymi lub ograniczenie praw, dyskryminacja, kradzież lub sfałszowanie tożsamości, strata finansowa, nieuprawione odwrócenie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne.

7. KONTROLA PRZETWARZANIA I STANU ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Powyższy rozdział reguluje system kontroli przetwarzania i stanu zabezpieczenia danych osobowych, kto jest odpowiedzialny za ich przeprowadzenie i jak często należy badać stan zabezpieczeń.

1. Nadzór i kontrolę nad ochroną danych osobowych przetwarzanych w Mercator Paweł Rokicki 96-315 Wiskitki Stary Drzewicz 3 sprawuje Administrator Danych Osobowych również w odniesieniu do danych osobowych przetwarzanych w systemach informatycznych służących do przetwarzania danych osobowych.
2. Administrator Danych Osobowych dokonuje czynności kontrolnych w ramach sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, zgodnie Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych.
3. Sprawdzenia dokonywane jest przez Administrator Danych Osobowych dla Prezesa Urzędu Ochrony Danych Osobowych, gdy ten na podstawie przysługujących mu kompetencji zwróci się o to do Administratora.
4. Administrator Danych Osobowych przeprowadza sprawdzenie w trybie:

4.1. sprawdzenia planowego - według opracowanego planu sprawdzeń;

4.2. sprawdzenia doraźnego - w przypadku nieprzewidzianym w planie sprawdzeń, w sytuacji powzięcia wiadomości o naruszeniu ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takiego naruszenia, niezwłocznie po powzięciu przez ADO takich informacji;

4.3. sprawdzenia w przypadku zwrócenia się o to przez Prezesa Urzędu Ochrony Danych Osobowych.

5. Administrator Danych Osobowych opracowuje plan sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
6. W toku sprawdzenia Administrator Danych Osobowych dokonuje i dokumentuje czynności, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz do opracowania sprawozdania.
7. Po zakończeniu sprawdzenia, Administrator Danych Osobowych przygotowuje sprawozdanie w tym zakresie. Sprawozdanie sporządzane jest w postaci elektronicznej albo w postaci papierowej.
8. Administrator Danych Osobowych ma prawo do kontroli podmiotów, którym powierzono

przetwarzanie danych osobowych w trybie określonym w Polityce Bezpieczeństwa, o ile w umowie o powierzeniu przetwarzania danych osobowych istnieją stosowne zapisy w tym zakresie.

9. Wzór sprawozdania ze sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych stanowi załącznik do Polityki Bezpieczeństwa

10. Wzór protokołu z kontroli lub czynności sprawdzających, stanowi załącznik do Polityki Bezpieczeństwa

8. OPIS STRUKTURY ZBIORÓW DANYCH

Dla każdego zidentyfikowanego zbioru danych zostaje wskazany opis struktury zbioru i zakres informacji gromadzonych w danym zbiorze.

Opisy poszczególnych pól informacyjnych gromadzonych w strukturze zbioru danych powinny jednoznacznie wskazywać jakie kategorie danych są w nich przechowywane.

Opis pola danych w przypadkach, gdy możliwa jest jednoznaczna interpretacja jego zawartości, powinien wskazywać nie tylko kategorie danych, ale również format zapisu.

ZALECA SIĘ sporządzenie opisu struktury zbiorów danych w formie tabeli, ponieważ jest to najbardziej czytelny sposób przedstawienia wymaganych informacji.

Opis struktury zbiorów danych stanowi załącznik do Polityki Bezpieczeństwa.

9. SPOSÓB PRZEPŁYWU DANYCH OSOBOWYCH POMIĘDZY SYSTEMAMI INFORMATYCZNYMI

1. W punkcie tym należy przedstawić sposób współpracy pomiędzy różnymi systemami informatycznymi oraz relacje, jakie istnieją pomiędzy danymi zgromadzonymi w zbiorach, do których systemy te są wykorzystywane.

1. Przepływ danych pomiędzy systemami zastosowanymi w celu przetwarzania danych osobowych może odbywać się w postaci przepływu jednokierunkowego lub przepływu dwukierunkowego.

2. Przesyłanie danych pomiędzy systemami i programami może odbywać się w sposób manualny, przy wykorzystaniu nośników zewnętrznych (np. CD, DVD, dysk wymienny, PenDrive itp.) lub w sposób półautomatyczny, przy wykorzystaniu funkcji eksportu/importu danych za pomocą teletransmisji (np. poprzez wewnętrzną sieć teleinformatyczną – WF MAG/Synergius – dwa oddzielne systemy (moduły programowe) przetwarzają dane zawarte w dwóch zbiorach pomiędzy którymi występuje przepływ danych). W przypadku pozostałych programów bezpośredni przepływ danych nie istnieje.

3. Przesyłanie danych może odbywać się zarówno w obrębie firmy, jak i na zewnątrz np. do firm, z którymi zawarto umowę o powierzeniu danych.

4. Dane osobowe przetwarzane firmie za pomocą oprogramowania przesyłane są pomiędzy poszczególnymi programami w następujący sposób:

- Program WF Mag generuje dane dla następujących modułów: magazyn, księgowość, faktury

- Dane w specjalnym formacie zawierające informacje zaszyfrowane osobowe przesyłane są do zewnętrznego biura rachunkowego

- Program Synergius generuje dane dotyczące klientów/zamawiających system CRM zintegrowany z pocztową mailową i programem handlowo-magazynowym.

5. Dane przechowywane są w wersji elektronicznej w systemach zabezpieczonych hasłem.

10. OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

1. Określenie obszaru pomieszczeń, w których przetwarzane są dane osobowe, powinno obejmować zarówno miejsca, w którym wykonuje się operacje na danych osobowych (wpisuje, modyfikuje, kopiuje), jak również miejsca, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe.

2. Wskazując na obszar przetwarzania danych należy uwzględnić także obszar, w którym przetwarzane są dane powierzone przez Administratora Danych odrębnym podmiotom.

Wykaz podmiotów, którym dane zostały powierzone, wraz ze wskazaniem obszaru przetwarzania danych znajduje się w załączniku do Polityki Bezpieczeństwa.

		Uwagi
pomieszczenia, w których przetwarzane są dane osobowe (wskazanie konkretnych nr pomieszczeń)	np. pokój nr 1, 2, 3, 4 sekretariat	
pomieszczenia, w których znajdują się komputery stanowiące element systemu informatycznego	np. pokój nr 1, 2	
Pomieszczenia, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające komputerowe nośniki informacji z kopiami zapasowymi danych, stacje komputerowe, serwery i inne urządzenia komputerowe)	np. pokój nr 1, 2, 3	
pomieszczenia, w których składowane są uszkodzone komputerowe nośniki danych (taśmy, dyski, płyty CD, dyski przenośne, uszkodzone komputery)	np. pokój 3	
pomieszczenia archiwum	np. pokój 4	

11. ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI IROZLICZALNOŚCI PRZETWARZANYCH DANYCH OSOBOWYCH

1. Rozdział ten powinien zawierać wykaz środków technicznych i organizacyjnych, które zostały zastosowane przez Administratora Danych w celu zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzania danych, a także dla zagwarantowania poufności, integralności i rozliczalności przetwarzanych danych osobowych.

Zestawienia zastosowanych środków technicznych i organizacyjnych przedstawiono w załączniku do Polityki Bezpieczeństwa.

12. ZAŁĄCZNIKI

Załącznik nr 1 – Inspektor Danych Osobowych Informacja

Załącznik nr 2 – Rejestr czynności przetwarzania danych

Załącznik nr 3 – Oszacowanie ryzyka związane z przetwarzaniem danych osobowych

Załącznik nr 4a – Wzór upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie umowy o pracę

Załącznik nr 4b – Wzór upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie innej umowy niż umowa o pracę

Załącznik nr 5 – Wzór oświadczenia o zobowiązaniu się do zachowania poufności

Załącznik nr 6 – Opis struktury zbiorów danych

Załącznik nr 7 – Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

Załącznik nr 8 – Wykaz podmiotów, którym Administrator Danych powierzył przetwarzanie danych osobowych

Załącznik nr 9 – Opis środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

Załącznik nr 10 –Wzór sprawozdania ze sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych

Załącznik nr 11 – Protokół z kontroli przetwarzania i stanu zabezpieczenia danych osobowych/czynności sprawdzających

Załącznik nr 12 - Zasady polityki czystego biurka

Dokument sporządzono:	**Pełen podpis Administratora Danych:**
Data: 25/05/2018 Miejsce: Wiskitki	

Załącznik nr 1 – Inspektor Danych Osobowych Informacja

Niniejszym, na podstawie Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych dalej: „Ustawa") Administrator Danych – Mercator Paweł Rokicki 96-315 Starowiskitki Stary Drzewicz 3

<u>Nie powołuję w firmie Mercator Paweł Rokicki</u>

Inspektora Danych Osobowych (IDO)

W celu oceny, czy powołanie jest niezbędne wzięto pod uwagę: skalę działalności, ilość zatrudnionych pracowników, rodzaj przetwarzanych danych osobowych, ilość przetwarzanych danych osobowych.

Uzasadnienie

Ponieważ:

a) przetwarzania danych osobowych firma nie dokonuje jako organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;

b) główna działalność administratora nie polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę; oraz główna działalność administratora nie polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10.

Administrator nie wyznacza inspektora ochrony danych.

....

DATA I PODPIS ADMINISTRATORA DANYCH

Załącznik nr 2 – Rejestr czynności przetwarzania danych

Rejestr czynności przetwarzania danych ujęty w zapisie tabelarycznym.

....

DATA I PODPIS ADMINISTRATORA DANYCH

Oszacowanie ryzyka związane z przetwarzaniem danych osobowych firmy Mercator Paweł Rokicki 96-315 Wiskitki Stary Drzewicz 3

1. Zbierane, posiadane i przetwarzane przez firmę zasoby informacyjne zawierają informacje należące do kategorii:

4 wrażliwe (zdrowie, dane genetyczne , pochodzenie , światopogląd) – **nie**
3 Finansowe (wynagrodzenie, konta bankowe , ubezpieczenia, status materialny)- **tak**
2 Behawioralne (informacje o nawykach i zwyczajach) **- nie**
1 Proste (dane osobowe i kontaktowe w celu realizacji umów i kontraktów)- **tak**

2.Prawdopodobieństwo wystąpienia danego zdarzenia oceniamy jako zdarzenie:
5 Pewne
4 Prawie pewne
3 Możliwe
2 Znikome
1 Nierealne

3. Wystąpienie danego zdarzenia dla osoby fizycznej, której dane są przetwarzane wiąże się dla niej ze stopniem dotkliwości:

5 Krytycznym - skutki zdarzenia są nieodwracalne
4 Znacznym - skutki zdarzenia będą odczuwane przez długi okres czasu
3 Średnim - skutki zdarzenia są krótkoterminowe do odwrócenia w krótkim okresie czasu
2 Umiarkowanym - zdarzenie skutkuje przejściowymi i względnie mało uciążliwymi skutkami
1 Minimalnym - osoba w żadnym stopniu nie odczuje skutków danego zdarzenia

Ryzyko nr 1

Dostęp do dokumentów w formie papierowej przez osobę nieuprawnioną.

Kategoria zajścia zdarzenia	znikoma
Podstawowe źródła ryzyka	1. włamanie 2. przypadkowe zniszczenie dokumentów 3. pożar 4. utrata dostępu do danych- zagubienie kluczy
zastosowane zabezpieczenia przed zdarzeniem	1. zamykana szafa, zamykany pokój z dokumentami , system alarmowy, monitoring budynku na zewnątrz 2. elektroniczna kopia dokumentów na komputerach zabezpieczonych hasłem 3. system alarmowy 4. zapasowy komplet kluczy
Uciążliwość zdarzenia	minimalna
Zalecane środki	1. brak potrzeby zwiększania środków zaradczych 2. rutynowa okresowa zmiana haseł dostępu do komputerów i zainstalowanych programów 3. brak potrzeby zwiększania środków zaradczych 4. wymiana zamków w przypadku wystąpienia zdarzenia

Ryzyko nr 2

Dostęp do dokumentów w formie elektronicznej przez osobę nieuprawnioną.

Kategoria zajścia zdarzenia	znikoma
Podstawowe źródła ryzyka	1. włamanie fizyczne, kradzież komputerów 2. przypadkowe skasowanie danych 3. pożar 4. utrata dostępu do danych, zgubienie haseł, wirus, włamanie do systemu przez hakera
zastosowane zabezpieczenia przed zdarzeniem	1. zamykany pokój , system alarmowy, monitoring budynku na zewnątrz 2. kopie zapasowe danych 3. system alarmowy 4. uruchomiona opcja odzyskiwania haseł, programy antywirusowe, szyfrowanie danych
Uciążliwość zdarzenia	minimalna
Zalecane środki	1. brak potrzeby zwiększania środków zaradczych 2. okresowe tworzenie kopii zapasowych 3. brak potrzeby zwiększania środków zaradczych 4. okresowa aktualizacja programów antywirusowych I zabezpieczających

....

DATA I PODPIS ADMINISTRATORA DANYCH

Załącznik nr 4a – Wzór upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie umowy o pracę

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Niniejszym, jako Administrator Danych w Mercator Paweł Rokicki 96-315 Starowiskitki Stary Drzewicz na podstawie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych, **upoważniam:**

Imię i nazwisko upoważnionego pracownika	
Zbiory danych objęte zakresem upoważnienia	**Dane pracowników/dane klientów**

Osoba upoważniona obowiązana jest przetwarzać dane osobowe zawarte w ww. zbiorach danych osobowych w zakresie i w sposób wymagany do wypełnienia obowiązków służbowych względem Administratora Danych.

Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz z przepisami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych, wydanymi na jej podstawie aktami wykonawczymi i obowiązującymi w Mercator Paweł Rokicki 96-315 Starowiskitki Stary Drzewicz 3 wewnętrznymi regulacjami w sprawie ochrony danych osobowych.

Naruszenie ww. obowiązków może skutkować poniesieniem odpowiedzialności karnej na podstawie przepisów określonych w Ustawie o ochronie danych osobowych oraz stanowi ciężkie naruszenie obowiązków pracowniczych, które może być podstawą rozwiązania umowy o pracę w trybie art. 52 Kodeksu Pracy.

Upoważnienie jest ważne do odwołania.

Data i podpis upoważniającego

Data i podpis osoby upoważnionej

Oświadczenie

Oświadczam, że zapoznałam/em się z obowiązującymi w zakresie ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi w Mercator Paweł Rokicki 96-315 Starowiskitki Stary Drzewicz 3 (w szczególności z Polityką Bezpieczeństwa). Przyjmuję do wiadomości zawarte w nich obowiązki w zakresie ochrony danych osobowych i zobowiązuję się do ich stosowania.

Świadoma/y jestem obowiązku ochrony danych osobowych na zajmowanym stanowisku i w zakresie udzielonego mi upoważnienia do przetwarzania danych osobowych, a w szczególności obowiązku zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu upoważnienia, a także po ustaniu zatrudnienia.

.....

Data i podpis osoby upoważnionej

Rozdzielnik 2 egz. w oryginale:
1 x oryginał dokumentacja kadrowa
1 x oryginał osoba upoważniona

Załącznik nr 4b – Wzór upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie innej umowy niż umowa o pracę

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Niniejszym, jako Administrator Danych Mercator Paweł Rokicki 96-315 Starowiskitki Stary Drzewicz 3, na podstawie Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych, **upoważniam:**

Imię i nazwisko upoważnionego	
Zbiory danych objęte zakresem upoważnienia	**Dane osób, z którymi zawarto umowy cywilnoprawne**

Osoba upoważniona obowiązana jest przetwarzać dane osobowe zawarte w ww. zbiorach danych osobowych w zakresie i w sposób wymagany do wypełnienia obowiązków służbowych względem Administratora Danych.

Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz z przepisami Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 r. poz. 922 ze zm.), wydanymi na jej podstawie aktami wykonawczymi i obowiązującymi w Mercator Paweł Rokicki 96-315 Starowiskitki Stary Drzewicz 3 wewnętrznymi regulacjami w sprawie ochrony danych osobowych.

Naruszenie ww. obowiązków może skutkować poniesieniem odpowiedzialności karnej na podstawie przepisów określonych w Ustawie o ochronie danych osobowych oraz odpowiedzialności cywilnej.

Upoważnienie jest ważne do odwołania.

Data i podpis upoważniającego

Data i podpis osoby upoważnionej

Oświadczenie

Oświadczam, że zapoznałam/em się z obowiązującymi w zakresie ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi w Mercator Paweł Rokicki 96-315 Starowiskitki Stary Drzewicz 3 (w szczególności z Polityką Bezpieczeństwa). Przyjmuję do wiadomości zawarte w nich obowiązki w zakresie ochrony danych osobowych i zobowiązuję się do ich stosowania.

Świadoma/y jestem obowiązku ochrony danych osobowych w związku z pełnioną przeze mnie funkcją i w zakresie udzielonego mi upoważnienia do przetwarzania danych osobowych, a w szczególności obowiązku zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu upoważnienia, a także po ustaniu stosunku prawnego łączącego mnie z Administratorem Danych.

……..
Data i podpis osoby upoważnionej

Rozdzielnik 2 egz. w oryginale:
1 x oryginał dokumentacja kadrowa
1 x oryginał osoba upoważniona

Załącznik nr 5 – Wzór oświadczenia o zobowiązaniu się do zachowania poufności

……………………., dnia ……………..

Oświadczenie o zobowiązaniu się do zachowania poufności

Ja niżej podpisana/y . . . . zamieszkała/y w . . . . zatrudniona/y na stanowisku . . . . zobowiązuję się zachować w tajemnicy informacje uzyskane w związku z …………………………….. Uzyskane informacje zachowam w poufności zarówno w trakcie zatrudnienia, jak i po jego ustaniu.

………………………………………….…………………..

Podpis

Załącznik nr 6 – Opis struktury zbiorów danych

Nr	Nazwa	Systemy informatyczne	Cel przetwarzania	Kategoria osób	Zakres przetwarzanych danych	Uwagi
1.	Dane pracowników	Program kadrowo płacowy, Płatnik	Realizacja obowiązków związanych z zatrudnieniem pracowników	Pracownicy	Dane niezbędne do obsługi procesu kadrowo płacowego	Firma zewnętrzna
2.	Dane osób wykonujących usługi na podstawie umów cywilnoprawnych	Program kadrowo płacowy, Płatnik	Realizacja obowiązków związanych z rozliczaniem współpracowników	Współpracownicy	Dane niezbędne do obsługi procesu płacowego	Firma zewnętrzna
3.	Dane osób reprezentujących klientów	konta mailowe pracowników na serwerze obsługującym pocztę firmową pliki tekstowe z tworzonymi umowami zapisane na dyskach twardych komputerów upoważnionych pracowników	Realizacja zamówień, prowadzenie sprawozdawczości finansowej oraz marketing własnych produktów	Osoby reprezentujące klientów	Imię, nazwisko, miejsce zatrudnienia, adres poczty elektronicznej, nr telefonu,	
4.	Dane osobowe niezbędne w procesie zamówień	Synerdius CRM	Zarządzanie procesami sprzedaży	Klienci	Imię, nazwisko, adres, nr telefonu,	
5.	Dane osobowe niezbędne w procesie obsługi kontrahenta	WF MAG	Prowadzenie ewidencji towarowo-wartościowej, księgowej, fakturowej	Kontrahenci	Dane teleadresowe kontrahenta	

Załącznik nr 7 – Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

Nr	Imię i nazwisko osoby upoważnionej	Data nadania upoważnienia	Data ustania upoważnienia	Indywidualny identyfikator wsystemie informatycznym	Nazwy zbiorów objętych zakresem upoważnienia
1.	Sylwia Rokicka	25/05/2018	25/05/2018		Dane osobowe/Dane klientów
2.	Anna Antończyk	25/05/2018	25/05/2018		Dane osobowe/Dane klientów
3.	Olga Gajownik	25/05/2018	25/05/2018		Dane klientów
4.	Łukasz Szczęśniak	25/05/2018	25/05/2018		Dane klientów
5.	Radosław Wójciku	25/05/2018	25/05/2018		Dane klientów
6.	Tomasz Wójcik	25/05/2018	25/05/2018		Dane klientów
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					

Załącznik nr 8 – Wykaz podmiotów, którym Administrator Danych powierzył przetwarzanie danych osobowych

	Adres / lokalizacja	Uwagi
Podmioty, którym Administrator Danych powierzył przetwarzanie danych osobowych	**Biuro Rachunkowe "Cedar" Cebulscy spółka jawna ul. Jaśminowa 7 96-300 Korytów adres biura: ul. 1-go Maja 17 lok. 14 96-300 Żyrardów**	

Załącznik nr 9 – Opis środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

ŚRODKI FIZYCZNE

Środek ochrony fizycznej	Zastosowano (TAK / NIE)	Uwagi
1. Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym **drzwiami zwykłymi** (niewzmacnianymi, nie przeciwpożarowymi).	**TAK**	
2. Zbiór danych osobowych przechowywany jest w pomieszczeniu, w którym okna zabezpieczone są za **szyb antywłamaniowych P4.**	**TAK**	
3. Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są w **system alarmowy przeciwwłamaniowy.**	**TAK**	
4. Dostęp do pomieszczeń, w których przetwarzany jest zbiory danych osobowych objęte są **systemem kontroli dostępu.**	**TAK**	
5. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych kontrolowany jest przez **system monitoringu z zastosowaniem kamer przemysłowych.**	**TAK**	
6. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych jest w czasie **nieobecności zatrudnionych** tam pracowników **nadzorowany .**	**TAK**	
7. Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej **niemetalowej szafie.**	**TAK**	
8. Zbiór danych osobowych w formie papierowej przechowywany jest w **zamkniętej metalowej szafie.**	**NIE**	
9. Zbiór danych osobowych w formie papierowej przechowywany jest **w zamkniętym sejfie lub kasie pancernej.**	**NIE**	
10. **Kopie zapasowe/archiwalne** zbioru danych osobowych przechowywane są w **zamkniętej niemetalowej szafie.**	**TAK**	

11. **Kopie zapasowe/archiwalne** zbioru danych osobowych przechowywane są **w zamkniętej metalowej szafie**.	**NIE**	
12. Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą **systemu przeciwpożarowego** i/lub **wolnostojącej gaśnicy.**	**TAK**	
13. Dokumenty zawierające dane osobowe **po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.**	**TAK**	

ŚRODKI TECHNICZNE

Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej	Zastosowano (TAK / NIE)	Uwagi
Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.	**TAK**	
Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.	**TAK**	
Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.	**TAK**	
Użyto system Firewall do ochrony dostępu do sieci komputerowej.	**TAK**	

ŚRODKI ORGANIZACYJNE

Środek organizacyjny	Zastosowano (TAK / NIE)	Uwagi
Do przetwarzania danych osobowych dopuszczono wyłącznie osoby posiadające upoważnienie nadane przez administratora danych	**TAK**	
Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych	**TAK**	
Opracowano i wdrożono Politykę Bezpieczeństwa	**TAK**	
Powołano Inspektora Ochrony Danych	**NIE**	
Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych	**TAK**	
Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego	**TAK**	
Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy	**TAK**	
Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym	**TAK**	
Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco	**TAK**	

Załącznik nr 10 - Wzór sprawozdania ze sprawdzenia zgodności przetwarzania danych osobowych zprzepisami o ochronie danych osobowych

Starowiskitki , ……..

miejscowość, data

SPRAWOZDANIE

ZE SPRAWDZENIA ZGODNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

z przepisami o ochronie danych osobowych

1. Administrator Danych: Mercator Paweł Rokicki 96-315 Wiskitki Stary Drzewicz 3
2. Wykaz czynności podjętych w toku sprawdzenia: ……

   ……

   ……

   ……

   ……
3. Data rozpoczęcia sprawdzenia:

   …….....
4. Data zakończenia sprawdzenia:

   …….....
5. Przedmiot i zakres sprawdzenia:

   …….....

   ……

   ……

   ……

   ……
6. Opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych: ……

   ……

   ……

……

……

7. Stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem: …..

……

……

……

……

……

……

……

……

8. Załączniki:

……

Podpis ADO

Załącznik nr 11 - Protokół z kontroli przetwarzania i stanu zabezpieczenia danych osobowych/ czynności sprawdzających

……..

miejscowość, data

PROTOKÓŁ

Z KONTROLI / CZYNNOŚCI SPRAWDZAJĄCYCH*

w zakresie ochrony danych osobowych

9. Nazwa kontrolowanej jednostki organizacyjnej: …….....
10. Zbiory danych osobowych, których przetwarzanie podlega kontroli: …….....
11. Data wykonania czynności kontrolnych: …….....
12. Imię i nazwisko oraz stanowisko osoby wykonującej czynności kontrolne: …….....
13. Imiona i nazwiska osób udzielających informacji dotyczących ochrony danych osobowych w kontrolowanej komórce organizacyjnej:…….…….
……..…..
……..

6. Ustalenia dokonane w trakcie czynności kontrolnych:……
……
……
……
……
……
……
7. Wnioski i zalecenia pokontrolne:
……
……
……
……
……
……

……..

(data i podpis osoby wykonującej czynności kontrolne)

……...

(data i podpis kierownika kontrolowanej kom. organizacyjnej)

Załącznik nr 12 - Zasady polityki czystych biurek

ZASADY POLITYKI CZYSTEGO BIURKA

Starowiskitki, dnia 25 maja 2018 r.

POLITYKA CZYSTEGO BIURKA

Mercator Paweł Rokicki 96-315 Starowiskitki Stary Drzewicz 3

1. Polityka czystego biurka jest częścią polityki bezpieczeństwa Mercator Paweł Rokicki 96-315 Starowiskitki Stary Drzewicz 3 i obowiązuje wszystkich pracowników zatrudnionych w Mercator Paweł Rokicki 96-315 Starowiskitki Stary Drzewicz 3
2. Przez pracownika należy rozumieć osobę, o której mowa w art. 2 Kodeksu pracy, zleceniobiorcę, praktykanta, osoby prowadzącą jednoosobową działalność gospodarczą współpracujące z Mercator Paweł Rokicki 96-315 Starowiskitki Stary Drzewicz 3
3. Pracownik:
   a) zobowiązany jest do przechowywania na biurku tylko tych dokumentów, które są mu potrzebne do wykonywania w danym momencie pracy;
   b) nie może przetrzymywać na biurku jedzenia oraz picia;
   c) po zakończonej pracy pracownik zobowiązany jest do zabezpieczenia dokumentów w zamykanej na klucz szafie;
   d) zobowiązany jest do niszczenia dokumentów niepotrzebnych w taki sposób, aby nie było możliwe odtworzenie zawartych w nich informacji, np. w niszczarce.
4. Zasady wymienione w niniejszej polityce obowiązują od 25 maja 2018 r.

Podpis ADO