

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBYWYCH

Firma Handlowo Usługowa „Elektrotechnika”

Zbigniew Rząsa

Spis treści

I. Informacje ogólne	4
II. Definicje	5
III. Dokumenty powiązane	6
IV. Cel i zakres Polityki Bezpieczeństwa	6
V. Obowiązki i odpowiedzialność.....	8
VI. Zarządzanie ochroną danych osobowych.....	9
VII. Szkolenia użytkowników.....	10
VIII. Upoważnienie do przetwarzania danych osobowych	10
IX. Ewidencja osób upoważnionych	11
X. Udostępnianie danych osobowych.....	11
XI. Dokonanie obowiązku informacyjnego.....	11
XII. Przetwarzanie danych osobowych oraz wymagania bezpieczeństwa	12
XIII. Polityka prywatności w serwisie internetowym	15
XIV. Postępowanie w sytuacji naruszenia bezpieczeństwa danych osobowych	15
XV. Zgodność.....	16
XVI. Postanowienia końcowe	16
Załącznik nr 1 Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych w firmie FHU ELEKTROTECHNIKA ZBIGNIEW RZAŚA	18
Załącznik nr 2 Ewidencja osób upoważnionych do przetwarzania danych osobowych.....	19
Załącznik nr 3 Oświadczenie użytkownika.....	20
Załącznik nr 4 Upoważnienie do przetwarzania danych osobowych (pracownicy/zleceniobiorcy).....	21
Załącznik nr 5 Odwołanie upoważnienia do przetwarzania danych osobowych	22
Załącznik nr 6 Wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe	23
Załącznik nr 7 Ustanowienie Administratora Bezpieczeństwa Informacji.....	25
Załącznik nr 8 Raport z naruszenia bezpieczeństwa danych osobowych.....	27
Załącznik nr 9 Struktura zbioru danych.....	29
Załącznik nr 10 Protokół ze sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych	28

I. Informacje ogólne

1. Głównym celem wprowadzenia Polityki Bezpieczeństwa jest zapewnienie zgodności działania firmy FHU Elektrotechnika Zbigniew Rząsa jako Administratora Danych Osobowych z przepisami prawa regulującymi kwestię administrowania i przetwarzania danych osobowych. Niniejsza Polityka Bezpieczeństwa opisuje w szczególności zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem.
2. Dokument Polityki Bezpieczeństwa został opracowany w oparciu o wytyczne zawarte w następujących aktach prawnych:
 - Ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r. poz. 922) ;
 - Rozporządzeniu 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 [rozporządzenie ogólne o ochronie danych];
 - Rozporządzeniu 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 (U. 2004 nr 100 poz. 1024),
3. Obszarem przetwarzania danych osobowych przez firmę FHU Elektrotechnika Zbigniew Rząsa jest każdorazowy adres siedziby firmy.
4. Ochrona danych osobowych realizowana jest poprzez stosowanie zabezpieczeń w postaci środków organizacyjnych, środków ochrony fizycznej oraz środków technicznych systemu informatycznego w ramach procedur zawartych w instrukcji zarządzania systemem informatycznym.
5. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w firmie FHU Elektrotechnika Zbigniew Rząsa rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych.
6. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów:
 - 1) Poufność danych - zapewnienie, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom,
 - 2) Integralność danych - zapewnienie, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
 - 3) Dostępność danych - zapewnienie osiągalności danych i możliwości ich wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot,
 - 4) Rozliczalność danych - zapewnienie, że działania podmiotu mogą być przy pisane w sposób jednoznaczny tylko temu podmiotowi,
 - 5) Autentyczność danych - zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana,
 - 6) Integralność systemu - rozumianą jako nienaruszalność systemu, niemożność jakiegokolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;

- 7) Zarządzanie ryzykiem - rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.
7. Administrator Danych Osobowych gromadzi przetwarza dane osobowe w następujących celach:
- 1) Wykonywanie obowiązków pracodawcy w zakresie zatrudnienia pracowników (dokumentacja i przebieg zatrudnienia oraz płace pracowników);
 - 2) Realizacja celu funkcjonowania firmy zgodnie z PKD. Prowadzenie sprzedaży oraz wypożyczalni narzędzi.

II. Definicje

1. Przez użyte w Polityce Bezpieczeństwa określenia należy rozumieć:
 - 1) Polityka Bezpieczeństwa - rozumie się przez to Politykę Bezpieczeństwa Ochrony Danych Osobowych w firmie FHU Elektrotechnika Zbigniew Rząsa;
 - 2) Elektrotechnika - firma FHU Elektrotechnika Zbigniew Rząsa, ul. Sienkiewicza 145, 39-400 Tarnobrzeg;
 - 3) Administrator Danych Osobowych - Administratorem Danych Osobowych w rozumieniu niniejszej Polityki Bezpieczeństwa jest firma FHU Elektrotechnika Zbigniew Rząsa, która reprezentowana jest przez Pana Zbigniewa Rząsę;
 - 4) Administrator Bezpieczeństwa Informacji - osoba, która dba o należyte zabezpieczenie danych osobowych oraz o kompleksowe zapewnianie u danego administratora danych przestrzegania przepisów o ochronie danych osobowych. Administratora Bezpieczeństwa Informacji powołuje Administrator Danych Osobowych;
 - 5) Ustawa - ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r. poz. 922);
 - 6) Rozporządzenie - 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) z późniejszymi zmianami;
 - 7) RODO - Rozporządzeniu 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 [rozporządzenie ogólne o ochronie danych]
 - 8) Dane osobowe - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;

- 9) Zbiór danych osobowych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
- 10) Baza danych osobowych - zbiór uporządkowanych powiązanych ze sobą tematycznie zapisanych np. w pamięci wewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze - rekordów lub obiektów, w których są zapisywane dane osobowe;
- 11) Usuwanie danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dotyczą.
- 12) Przetwarzanie danych - rozumie się przez to jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
- 13) System informatyczny - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
- 14) Bezpieczeństwo systemu informatycznego - wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed nieuprawnionym przetwarzaniem danych;
- 15) Administrator Systemu Informatycznego - osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych (może to być administrator sieci lokalnej, systemu operacyjnego, bazy danych itp.).
- 16) Użytkownik - rozumie się przez to osobę wyznaczoną i upoważnioną przez Administratora danych do przetwarzania danych osobowych, przeszkoloną w zakresie ochrony tych danych.
- 17) Stacja robocza - stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie.

III. Dokumenty powiązane

Dokumentem powiązanim z Polityką bezpieczeństwa przetwarzania danych osobowych w firmie Elektrotechnika jest, zgodnie z wymogami § 3 ust. 1 Rozporządzenia, Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w firmie Elektrotechnika

IV. Cel i zakres Polityki

1. Ustawa o ochronie danych osobowych nakłada na Administratora Danych obowiązek stosowania odpowiednich środków technicznych i organizacyjnych zapewniających

ochronę przetwarzanych danych osobowych oraz zabezpieczenie ich między innymi przed udostępnieniem osobom nieupoważnionym, przetwarzaniem z naruszeniem ustawy, a także zmianą, utratą, uszkodzeniem lub zniszczeniem. Celem niniejszej Polityki Bezpieczeństwa przetwarzania danych osobowych jest opracowanie optymalnych i zgodnych z wymogami prawa zasad przetwarzania danych, których zbieranie i przetwarzanie jest niezbędne dla realizacji zadań firmy Elektrotechnika.

2. W firmie Elektrotechnika przetwarzane są przede wszystkim dane osobowe pracowników firmy oraz osób współpracujących na podstawie umów cywilnoprawnych. Firma Elektrotechnika, w związku z realizacją zadań, przetwarza także dane osobowe klientów sklepu, serwisu oraz wypożyczalni. Wykaz poszczególnych zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych w firmie Elektrotechnika stanowi załącznik nr 1 do Polityki Bezpieczeństwa.
3. Dane osobowe we wskazanych powyżej zbiorach danych są przetwarzane i składowane zarówno w postaci dokumentacji tradycyjnej jak i elektronicznej.
4. Politykę Bezpieczeństwa stosuje się przede wszystkim do:
 - 1) Wszystkich informacji dotyczących danych pracowników firmy Elektrotechnika oraz osób współpracujących na podstawie umów cywilnoprawnych, w tym danych osobowych i treści zawieranych umów.
 - 2) Wszystkich danych kandydatów do pracy zbieranych na etapie rekrutacji.
 - 3) Wszystkich informacji dotyczących danych klientów firmy Elektrotechnika.
 - 4) Informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych.
 - 5) Rejestru osób dopuszczonych do przetwarzania danych osobowych.
 - 6) Innych dokumentów zawierających dane osobowe.
5. Zakres ochrony danych osobowych określony w Polityce Bezpieczeństwa ma zastosowanie do systemów informatycznych firmy Elektrotechnika, w których są przetwarzane dane osobowe, a w szczególności do:
 - 1) Wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie.
 - 2) Wszystkich lokalizacji - pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie.
 - 3) Wszystkich osób świadczących pracę bądź usługi cywilnoprawne na rzecz Administratora Danych Osobowych, które uzyskały upoważnienie do przetwarzania danych osobowych

6. Dla zapewnienia bezpieczeństwa osób fizycznych lub ochrony mienia lub kontroli jakości wykonywanych usług lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić firmę na szkodę, Administrator prowadzi szczególny nadzoru nad obiektami będącymi w użytkowaniu w postaci środków technicznych umożliwiających rejestrację obrazu (monitoring wizyjny) z wyłączeniem pomieszczeń socjalnych, w szczególności higieniczno-sanitarnych, szatni oraz stołówek. Dane z monitoringu wizyjnego usuwane są automatycznie po upływie 30 dni od zarejestrowania.
7. Do stosowania zasad określonych w Polityce Bezpieczeństwa zobowiązani są wszyscy Użytkownicy danych, w tym w szczególności pracownicy firmy Elektrotechnika, zleceniobiorcy, stażyści oraz wszelkie inne osoby mające dostęp do informacji podlegających ochronie.

V. Obowiązki i odpowiedzialność

1. Do najważniejszych obowiązków Administratora Danych realizowanych przez Administratora Bezpieczeństwa Informacji należy:
 - 1) Organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych oraz innych przepisów regulujących zasady bezpieczeństwa i ochrony danych osobowych;
 - 2) Zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki Bezpieczeństwa;
 - 3) Wydawanie i anulowanie upoważnień do przetwarzania danych osobowych;
 - 4) Przeprowadzanie szkoleń użytkowników przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe;
 - 5) Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
 - 6) Prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych;
 - 7) Nadzór nad bezpieczeństwem danych osobowych;
 - 8) Kontrola działań pracowników pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
 - 9) Inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych;
 - 10) Bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych;
 - 10) Optymalizację wydajności systemu informatycznego, baz danych, instalacje i konfiguracje sprzętu sieciowego i serwerowego;
 - 11) Instalacje i konfiguracje oprogramowania systemowego, sieciowego, oprogramowania bazodanowego;
 - 12) Konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz bazodanowym zabezpieczającym dane chronione przed nieupoważnionym dostępem;
 - 13) Współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych;

- 14) Zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego;
 - 15) Przeciwdziałanie próbom naruszenia bezpieczeństwa informacji;
 - 16) Zmiana lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń;
 - 17) Zarządzanie licencjami oraz procedurami ich dotyczącymi;
 - 18) Prowadzenie profilaktyki antywirusowej.
2. Do najważniejszych obowiązków osób upoważnionych do przetwarzania danych osobowych należy:
- 1) Znajomość, zrozumienie i stosowanie w możliwie największym zakresie wszelkich dostępnych środków ochrony danych osobowych oraz uniemożliwienie osobom nieuprawnionym dostępu do swojej stacji roboczej;
 - 2) Przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami prawa oraz przyjętymi regulacjami;
 - 3) Postępowania zgodnie z ustalonymi regulacjami wewnętrznymi dotyczącymi przetwarzania danych osobowych;
 - 4) Zachowania w tajemnicy danych osobowych, do których uzyskały dostęp oraz informacji o sposobach ich zabezpieczenia;
 - 5) Ochrony danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem;
 - 6) Informowania Administratora Danych Osobowych o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe;
 - 7) Zapoznanie się z Polityką Bezpieczeństwa przetwarzania danych osobowych oraz Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

VI. Zarządzanie ochroną danych osobowych

1. Za bieżącą, operacyjną ochronę danych osobowych odpowiada każda osoba przetwarzająca te dane w zakresie zgodnym z upoważnieniem oraz rolą sprawowaną w procesie przetwarzania danych.
2. Dostęp do danych osobowych powinien być przyznawany zgodnie z zasadą wiedzy koniecznej.
3. Każda z osób mająca styczność z danymi osobowymi jest zobowiązana do ochrony danych osobowych oraz przetwarzania ich w granicach udzielonego jej upoważnienia.
4. Należy zapewnić poufność, integralność i rozliczalność przetwarzanych danych osobowych.

5. Należy stosować adekwatny do zmieniających się warunków i technologii poziom bezpieczeństwa przetwarzania danych osobowych.
6. Dane osobowe powinny być chronione przed nieuprawnionym dostępem i modyfikacją.
7. Dane osobowe należy przetwarzać wyłącznie za pomocą autoryzowanych urządzeń służbowych.
8. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane na mocy art. 37 Ustawy. Upoważnienia wydawane są indywidualnie przez Administratora Danych Osobowych.

VII. Szkolenia użytkowników

1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.
2. Za przeprowadzenie szkolenia odpowiada Administrator Danych Osobowych.
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz Polityką Bezpieczeństwa danych i Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych obowiązującymi u Administratora Danych. Po zaznajomieniu się z powyższymi regulacjami, użytkownik, przed dopuszczeniem do przetwarzania danych, powinien zobowiązać się do ich przestrzegania przez podpisanie oświadczenia użytkownika, stanowiącego załącznik nr 3 do Polityki Bezpieczeństwa.

VIII. Upoważnienie do przetwarzania danych osobowych

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane na mocy art. 37 Ustawy.
2. Upoważnienia są wydawane indywidualnie przed rozpoczęciem przetwarzania danych osobowych przez Administratora Danych Osobowych.
3. W celu otrzymania przez Użytkownika upoważnienia do przetwarzania danych osobowych, należy dostarczyć do Administratora Danych podpisane oświadczenie użytkownika.
4. Na podstawie otrzymanego oświadczenia Administrator Danych Osobowych upoważnia Użytkownika do przetwarzania danych osobowych i wydaje upoważnienie do przetwarzania danych osobowych sporządzane wg wzoru stanowiącego załącznik nr 4 i 5 do Polityki Bezpieczeństwa.

5. Upoważnienie może być w każdym czasie odwołane przez Administratora Danych Osobowych. Oświadczenie o odwołaniu upoważnienia do przetwarzania danych osobowych powinno być sporządzone na piśmie. Upoważnienie do przetwarzania danych osobowych wygasa z chwilą ustania przesłanki będącej podstawą wydania upoważnienia, w tym w szczególności wygaśnięcia stosunku pracy lub umowy cywilnoprawnej łączącej Użytkownika z Administratorem Danych Osobowych.

IX. Ewidencja osób upoważnionych

Ewidencja osób upoważnionych do przetwarzania danych osobowych w firmie Elektrotechnika jest prowadzona przez Administratora Danych zgodnie ze wzorem formularza stanowiącym załącznik nr 2 do Polityki Bezpieczeństwa przetwarzania danych osobowych.

X. Udostępnianie danych osobowych

1. Dane osobowe mogą być udostępniane wyłącznie podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa oraz osobom, których dotyczą.
2. Udostępnianie danych osobowych może nastąpić wyłącznie za zgodą Administratora Danych Osobowych.
3. Informacje zawierające dane osobowe powinny być przekazywane uprawnionym podmiotom lub osobom za potwierdzeniem odbioru listem poleconym za pokwitowaniem odbioru lub innym bezpiecznym sposobem, określonym wymogiem prawnym lub umową.
4. Udostępniając dane osobowe, należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

XI. Dokonanie obowiązku informacyjnego

1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, w wypadkach przewidzianych Ustawą należy poinformować tę osobę o:
 - 1) Pełnej nazwie firmy Elektrotechnika i adresie siedziby;
 - 2) Celu zbierania danych, a w szczególności o znanych w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych;
 - 3) Prawie dostępu do swoich danych oraz ich poprawiania;
 - 4) Dobrowolności lub obowiązku podania danych - jeżeli taki obowiązek istnieje, o jego podstawie prawnej;

XII. Przetwarzanie danych osobowych oraz wymagania bezpieczeństwa.

1. Dane osobowe mogą być przetwarzane wyłącznie w obszarze przetwarzania danych osobowych, na które składają się pomieszczenia firmowe, z wyjątkiem sytuacji udostępnienia danych osobowych lub powierzenia przetwarzania danych osobowych. Szczegółowy wykaz pomieszczeń tworzących obszar przetwarzania danych osobowych znajduje się w załączniku nr 7 do Polityki Bezpieczeństwa.
2. Dane osobowe w firmie Elektrotechnika przetwarzane są przy zastosowaniu zabezpieczeń zapewniających ich ochronę w postaci środków organizacyjnych, technicznych i środków ochrony fizycznej.
3. Dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych stosuje się następujące środki:
 - A. Środki organizacyjne:
 - wdrożenie Polityki bezpieczeństwa przetwarzania danych osobowych oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
 - ustalona, indywidualna procedura udzielania upoważnień przez Administratora Danych poprzedzonego szkoleniem z zakresu przepisów i zasad ochrony danych osobowych;
 - prowadzenie ewidencji osób uprawnionych do przetwarzania danych osobowych,
 - procedura postępowania w sytuacji naruszenia ochrony danych osobowych;
 - konieczność składania deklaracji poufności przez Użytkowników danych;
 - procedury przechowywania zbiorów danych;
 - B. Środki techniczne:
 - Zbiory danych osobowych przetwarzane są wyłącznie na autoryzowanym sprzęcie służbowym;
 - Stacje robocze wyposażone są w indywidualną ochronę antywirusową;
 - Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
 - C. Środki ochrony fizycznej:
 - Pomieszczenia, w których znajdują się zbiory danych osobowych, są zamykane na klucz, a dostęp do nich odbywa się wyłącznie w obecności pracowników firmy Elektrotechnika;
 - Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy;
 - Drzwi zwykle (niewzmacniane, nie przeciwpożarowe) do pomieszczeń, w których przetwarzane są dane osobowe znajdują się wewnątrz budynku w strefie ograniczonego dostępu;
 - Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej niemetalowej szafie;
 - Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej niemetalowej szafie;
 - Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek.

4. Osobie, której dane będą przetwarzane przez firmę Elektrotechnika, przysługuje prawo do kontroli przetwarzania tych danych, a w szczególności prawo do informacji o:
 - a) fakcie przetwarzania danych jej dotyczących;
 - b) pełnej nazwie i adresie siedziby Administratora Danych Osobowych;
 - c) celu, zakresie i sposobie przetwarzania danych (środkach przy pomocy których dane są przetwarzane);
 - d) dacie, od kiedy dane są przetwarzane przez Administratora Danych Osobowych (dacie włączenia do zbioru) oraz podania w powszechnie zrozumiałej formie treści tych danych;
 - e) źródle danych, chyba że Administrator Danych Osobowych zobowiązany jest do zachowania w tym zakresie tajemnicy;
 - f) sposobie udostępniania danych oraz odbiorcach lub kategoriach odbiorców, którym dane są udostępniane;
 - g) żądania uzupełnienia, uaktualnienia, sprostowania, czasowego lub stałego wstrzymania przetwarzania danych lub ich usunięcia;
 - h) wniesienia do Administratora Danych Osobowych sprzeciwu wobec przetwarzania przez niego danych w celach marketingowych lub przekazania ich innemu administratorowi.

5. Prawa osób, których dane osobowe są przetwarzane:
 - a) Każda osoba, której dane osobowe są przetwarzane przez Administratora, ma prawo żądać od Administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, każda osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.
 - b) W zgłoszenia żądania w zakresie sprostowania danych osobowych, należy złożyć odpowiednie żądanie w formie pisemnej bezpośrednio na adres siedziby firmy Elektrotechnika lub poprzez adres elektroniczny email: poczta@elektrotechnika.org.
 - c) Każda osoba, której dane osobowe są przetwarzane ma prawo do uzyskania informacji od Administratora, czy i w jakim zakresie przetwarzane są jego dane osobowe, a także informacji o celu i zakresie przetwarzania jego danych osobowych.
 - d) Każda osoba, której dane osobowe są przetwarzane przez Administratora, ma prawo złożenia żądania wobec Administratora, w przedmiocie niezwłocznego usunięcia dotyczących tej osoby danych osobowych. W takim przypadku Administrator bez zbędnej zwłoki usunie dane osobowe osoby, która zgłosiła takie żądanie, chyba że obowiązek przetwarzania danych osobowych takiej osoby przez Administratora wynika z innych przepisów obowiązującego prawa.
 - e) Administrator ma prawo odmówić żądaniu w zakresie usunięcia danych osobowych także w przypadku, gdy wykaże, że przetwarza dane osobowe określonych osób dla celów archiwalnych w interesie publicznym. W takim przypadku Administrator poinformuje pisemnie osobę, która zgłosiła takie żądanie, o odmowie usunięcia danych osobowych, wskazując powody odmowy oraz podstawę prawną takiego działania.
 - f) Każda osoba, które dane osobowe są przetwarzane przez Administratora ma prawo w dowolnym momencie cofnąć zgodę na przetwarzanie danych osobowych dotyczących tej osoby, z zastrzeżeniem odmiennych postanowień niniejszej Polityki, które w określonych sytuacjach umożliwiają Administratorowi dalsze przetwarzanie danych osobowych, w szczególności powołując się na cele archiwalne oraz statystyczne.

- g) Wycofanie zgody na przetwarzanie danych osobowych nie ma wpływu na zgodność z prawem przetwarzania danych osobowych przez Administratora, które nastąpiło na podstawie zgody na przetwarzanie danych osobowych przed jej wycofaniem.
- h) Każda osoba, której dane osobowe są przetwarzane przez Administratora, ma prawo żądać od Administratora ograniczenia przetwarzania jej danych osobowych w każdym przypadku gdy:
- kwestionuje prawidłowość przetwarzanych jej danych osobowych – ograniczenie następuje na okres pozwalający na weryfikację przez Administratora sprawdzenie prawidłowości tych danych osobowych;
 - przetwarzanie danych osobowych jest niezgodne z prawem, a osoba fizyczna, której dane dotyczą, sprzeciwia się usunięciu jej danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
 - Administrator nie potrzebuje już danych osobowych celem ich przetwarzania, ale dane osobowe są potrzebne osobie, której dane osobowe są przetwarzane do ustalenia, dochodzenia lub obrony jego roszczeń;
 - Osoba, której dane osobowe są przetwarzane wniosła sprzeciw wobec przetwarzania danych osobowych przez Administratora – do czasu stwierdzenia oraz zweryfikowania przez Administratora czy prawnie uzasadnione podstawy po stronie Administratora w zakresie przetwarzania danych osobowych określonej osoby są nadrzędne wobec podstaw sprzeciwu tej osoby, która wniosła sprzeciw.
- i) W razie uchylecia ograniczenia przetwarzania danych osobowych, Administrator informuje o tym pisemnie osobę fizyczną, wobec której danych osobowych nastąpiło ograniczenia przetwarzania.
- j) Osoba fizyczna, której dane osobowe są przetwarzane przez Administratora ma prawo w dowolnym momencie wnieść sprzeciw z przyczyn związanych z jego szczególną sytuacją, wobec przetwarzania jego danych osobowych przez Administratora.
- k) W razie wniesienia sprzeciwu, Administratorowi nie wolno już przetwarzać danych osobowych tej osoby fizycznej, która wniosła sprzeciw, chyba że Administrator wykaże istnienie ważnych, prawnie uzasadnionych podstaw do dalszego przetwarzania danych osobowych tej osoby fizycznej, która wniosła sprzeciw, które są nadrzędne wobec partykularnych interesów osoby fizycznej, która wniosła sprzeciw bądź przetwarzanie danych osobowych osób fizycznych jest niezbędne do wykonywania przez Administratora zadań realizowanych w interesie publicznym.
- l) Powyższe ograniczenie nie dotyczy przetwarzania danych osobowych dla celów marketingowych, a w takiej sytuacji w razie wniesienia sprzeciwu, dane osobowe nie mogą już dalej być przetwarzane przez Administratora.
- m) Każda osoba, której dane osobowe są przetwarzane przez Administratora ma prawo żądać, aby jego dane osobowe przetwarzane przez Administratora zostały przekazane przez Administratora innemu podmiotowi (administratorowi), o ile jest to technicznie możliwe.

XIII. Polityka prywatności w serwisie internetowym.

Dane przekazywane podczas korzystania z serwisu internetowego <http://elektrotechnika.org> nie są udostępniane podmiotom trzecim. Nie przekazujemy i nie sprzedajemy zgromadzonych danych osobowych Użytkowników innym osobom lub podmiotom.

Zastrzegamy prawo udostępnienia danych Użytkownika uprawnionym organom (policja, prokuratura) – zgodnie z obowiązującymi przepisami prawa oraz instytucjom zajmującym się dochodzeniem należności, w tym przedsiębiorcom zajmującym się windykacją i obrotem wierzytelnościami oraz ich pełnomocnikom, z zachowaniem wymogów określonych właściwymi przepisami dotyczącymi ochrony danych osobowych.

W serwisie internetowym <http://elektrotechnika.org> wykorzystujemy pliki Cookies.

Pliki cookies to dane informatyczne, w szczególności pliki tekstowe, które są zapisywane przez serwer na komputerze Użytkownika niniejszego Serwisu. Pliki te pozwalają rozpoznać urządzenie Użytkownika i odpowiednio wyświetlić stronę internetową dostosowaną do jego indywidualnych preferencji.

W ramach Serwisu wykorzystywane są pliki cookies sesyjne - są plikami tymczasowymi, przechowywanymi w urządzeniu końcowym Użytkownika do czasu opuszczenia strony lub wyłączenia oprogramowania (przeglądarki internetowej);

Użytkownicy Serwisu mogą dokonać zmiany ustawień w zakresie plików cookies.

Przeglądarka internetowa umożliwia usunięcie plików cookies. Możliwe jest także automatyczne blokowanie plików cookies. Ograniczenia stosowania plików cookies mogą wpłynąć na niektóre funkcjonalności dostępne na stronach internetowych Serwisu.

XIV. Postępowanie w sytuacji naruszenia bezpieczeństwa danych osobowych

1. Każdy użytkownik w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest o tym poinformować Administratora Danych.
2. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
 - 1) Niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;
 - 2) Niewłaściwe zabezpieczenie sprzętu, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;

- 3) Rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości;
- 4) Dokumentuje prowadzone postępowania.
5. W przypadku stwierdzenia incydentu (naruszenia), Administrator Danych prowadzi postępowanie wyjaśniające, w toku którego:
 - 1) Ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały;
 - 2) Zabezpiecza ewentualne dowody;
 - 3) Ustala osoby odpowiedzialne za naruszenie;
 - 4) Podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody);
 - 5) Inicjuje działania dyscyplinarne;
 - 6) Wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości;
 - 7) Dokumentuje prowadzone postępowania zgodnie ze wzorem Raportu z naruszenia bezpieczeństwa danych osobowych stanowiących załącznik nr 10 do Polityki Bezpieczeństwa.

XV. Zgodność

Niniejsza Polityka powinna być aktualizowana wraz ze zmieniającymi się przepisami prawnymi o ochronie danych osobowych oraz zmianami faktycznymi w ramach działalności firmy Elektrotechnika, które mogą powodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne lub nieadekwatne.

XVI. Postanowienia końcowe

1. Administrator Danych ma obowiązek zapoznać z treścią Polityki każdego użytkownika.
2. Wszystkie regulacje dotyczące systemów informatycznych, określone w Polityce dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiegokolwiek innej formie.
3. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Polityce.
4. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.

5. Kara dyscyplinarna orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z ustawą oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
6. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy ustawy oraz rozporządzenia.

Załącznik nr 1

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych w firmie Elektrotechnika

L.p.	Nazwa zbioru danych osobowych	Podstawa prawna funkcjonowania zbioru	Forma prowadzenia	Zastosowany program komputerowy	Lokalizacja bazy danych	Miejsce przetwarzania danych
1.	DANE OSOBOWE PRACOWNIKÓW	Ustawa z dnia 26 czerwca 1974 r. Kodeks Pracy, Ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych, Ustawa z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych.	Dokumentacja w formie papierowej i elektronicznej	Płatnik	Pomieszczenie księgowej/ Stacje robocze	Pomieszczenie księgowej
2.	DANE KLIENTÓW SKLEPU	Ustawa z dnia 6 marca 2018 r. - Prawo przedsiębiorców	Dokumentacja w formie papierowej i elektronicznej	Motofirma, WfMag, Thunderbird	Pomieszczenia biura, stanowisko sprzedaży/ Stacje robocze, serwer	Pomieszczenia biura, stanowisko sprzedaży
3.	DANE KLIENTÓW WYPOŻYCZALNI	Ustawa z dnia 6 marca 2018 r. - Prawo przedsiębiorców	Dokumentacja w formie papierowej		Pomieszczenia biura	Pomieszczenia biura
4.	MONITORING WIZYJNY	Ustawa o ochronie danych osobowych: art. 23 ust. 1 pkt 5	Rejestrator wideo		Pomieszczenia biura	Pomieszczenia biura

Załącznik nr 2

Ewidencja osób upoważnionych do przetwarzania danych osobowych

L.p.	Numer upoważnienia	Nazwa zbioru danych	Nazwisko i imię osoby upoważnionej	Data nadania upoważnienia	Zakres upoważnienia	Data wygaśnięcia / cofnięcia upoważnienia	UWAGI (przyczyna cofnięcia uprawnień)

Załącznik nr 3 Oświadczenie użytkownika

(Data, miejscowość)

(Imię i nazwisko Użytkownika)

(Adres zamieszkania)

Ja niżej podpisana/-y oświadczam, iż:

Zostałam/-em przeszkolona/-y w zakresie ochrony danych osobowych i znana jest mi treść ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych Dz.U. 1997 Nr 133 poz. 883 z późn. zm. oraz regulacje zawarte w Polityce bezpieczeństwa przetwarzania danych osobowych oraz Instrukcji zarządzania systemem informatycznym w firmie FHU ELEKTROTECHNIKA ZBIGNIEW RZAŚA oraz zobowiązuję się do ich przestrzegania.

Jednocześnie zobowiązuję się:

1. zachować w tajemnicy powierzone mi do przetwarzania dane osobowe;
2. chronić dane osobowe przed dostępem do nich osób do tego nieupoważnionych, zabezpieczać je przed zniszczeniem i nielegalnym ujawnieniem.

Znana jest mi odpowiedzialność karna za naruszenie ww. ustawy (art. 49-54).

*(podpis Administratora Danych lub
osoby reprezentującej Administratora Danych)*

(podpis Użytkownika)

Załącznik nr 4 Upoważnienie do przetwarzania danych osobowych

(Data, miejscowość)

Z dniem na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2015 nr 0 poz. 2135 - tekst jednolity z późn. zm.)

upoważniam Panią / Pana
(imię i nazwisko)

do przetwarzania danych osobowych w zbiorze o nazwie:

w systemie tradycyjnym i/lub informatycznym

w zakresie ich zbierania, utrwalania, przechowywania, opracowywania, zmieniania, udostępniania i usuwania

w związku z wykonywaniem obowiązków wynikających z umowy o pracę / umowy cywilnoprawnej* zawartej firmą FHU ELEKTROTECHNIKA ZBIGNIEW RZĄSA.

Przyjmuję do wiadomości i przestrzegania oraz zobowiązuję się do zachowania w tajemnicy tych danych osobowych oraz sposobów ich zabezpieczeń.

(podpis osoby reprezentującej Administratora Danych)

Oświadczam, że zobowiązuję się do zachowania w tajemnicy tych danych osobowych oraz sposobów ich zabezpieczeń.

(podpis Użytkownika)

Załącznik nr 5

Odwołanie upoważnienia do przetwarzania danych osobowych

na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz U. 2015 nr 0 poz. 2135- tekst jednolity z późn. zm.)

z dniem.....odwołuję upoważnienie

nr

Dla Pani/Pana

(imię i nazwisko Użytkownika)

(podpis Użytkownika)

(podpis osoby reprezentującej Administratora Danych)

Załącznik nr 6

Wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe

Polityka obowiązuje w firmie FHU ELEKTROTECHNIKA ZBIGNIEW RZAŚA, w pomieszczeniach, w których przetwarzane są dane osobowe, a których wykaz został zamieszczony poniżej.

Firma FHU ELEKTROTECHNIKA ZBIGNIEW RZAŚA ma siedzibę przy ul. Sienkiewicza 145, 39-400 Tarnobrzeg.

1.	Wykaz pomieszczeń, w których przetwarzane są dane osobowe (wskazanie konkretnych nr pomieszczeń)	Pomieszczenie biurowe, pomieszczenie sprzedaży
2.	Wykaz pomieszczeń, w których znajdują się stacje robocze stanowiące element systemu informatycznego (jednostki robocze)	Pomieszczenie biurowe, pomieszczenie sprzedaży
3.	Wykaz pomieszczeń, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające komputerowe nośniki informacji z kopiami zapasowymi danych, stacje komputerowe)	Pomieszczenie biurowe
4.	Wykaz programów, w których przetwarzane są dane osobowe	OpenOffice, Motofirma, WfMag, Thunderbird, Płatnik
5.	Informacje dotyczące pomieszczeń, w których przetwarzane są dane osobowe oraz ich zabezpieczeń.	Szafy zamykane na klucz, Serwer z hasłem zmienianym nie rzadziej niż raz na 30 dni, komputery z indywidualnymi hasłami - zmiana nie rzadziej niż raz na 60 dni.

Załącznik nr 7 Ustanowienie Administratora Bezpieczeństwa Informacji

Niniejszym, na podstawie art. 36a ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922 ze zm. dalej: „Ustawa”) działając w imieniu Administratora Danych – firmy FHU ELEKTROTECHNIKA ZBIGNIEW RZAŚA z siedzibą w Tarnobrzegu, 39-400, ul. Sienkiewicza 145.

powołuję

Panią/Pana

na stanowisko Administratora Bezpieczeństwa Informacji (ABI) w firmie ELEKTROTECHNIKA ZBIGNIEW RZAŚA.

Jednocześnie, na podstawie art. 37 Ustawy upoważniam Panią/Pana do przetwarzania danych osobowych we wszystkich zbiorach Administratora Danych w zakresie niezbędnym dla należytego wykonywania funkcji Administratora Bezpieczeństwa Informacji.

Zakres obowiązków oraz warunki pełnienia funkcji Administratora Bezpieczeństwa Informacji określone są Ustawą o ochronie danych osobowych z dnia 29 sierpnia 1997 roku oraz dokumentacją z zakresu ochrony danych osobowych.

(podpis osoby reprezentującej Administratora Danych)

Załącznik nr 8 Raport z naruszenia bezpieczeństwa danych osobowych

(Data, miejscowość)

1. Data:..... r. Godzina:.....
2. Osoba powiadamiająca o zaistniałym zdarzeniu:
(imię, nazwisko, stanowisko służbowe, nazwa użytkownika - jeśli występuje)
3. Lokalizacja zdarzenia (np. nr pokoju, nazwa pomieszczenia):
4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące: .
5. Przyczyny wystąpienia zdarzenia:
6. Podjęte działania:
7. Postępowanie wyjaśniające:

(podpis osoby reprezentującej Administratora Danych)

Załącznik nr 9 Struktura zbiorów danych

Struktura zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych dla zbiorów w formie papierowej oraz systemów informatycznych, stosowanych w firmie FHU ELEKTROTECHNIKA ZBIGNIEW RZAŚA przedstawia się w sposób następujący:

DANE OSOBOWE PRACOWNIKÓW I ZLECENIOBIORCÓW

ZBIORY W FORMIE PAPIEROWEJ I ELEKTRONICZNEJ

- 1) Imię,
- 2) Nazwisko,
- 3) Data i miejsce urodzenia,
- 4) Adres zamieszkania (kod pocztowy, miejscowość, ulica, nr domu/mieszkania),
- 5) PESEL,
- 6) Seria i numer dokumentu tożsamości,
- 7) Nazwa banku i nr konta bankowego,
- 8) Nazwa i rok ukończenia szkoły,
- 9) Historia zatrudnienia.

DANE OSOBOWE KLIENTÓW SKLEPU

ZBIORY W FORMIE PAPIEROWEJ I ELEKTRONICZNEJ

- 1) Imię,
- 2) Nazwisko,
- 3) Adres zamieszkania (kod pocztowy, miejscowość, ulica, nr domu/mieszkania),
- 4) NIP,
- 5) Tel.,
- 6) Fax,
- 7) Adres e-mail,
- 8) Tel. komórkowy.

DANE OSOBOWE KLIENTÓW WYPOŻYCZALNI
ZBIORY W FORMIE PAPIEROWEJ

- 1) Imię,
- 2) Nazwisko,
- 3) Adres zamieszkania (kod pocztowy, miejscowość, ulica, nr domu/mieszkania),
- 4) Seria i numer dokumentu tożsamości,
- 5) Adres e-mail,
- 6) Tel. komórkowy.

Załącznik nr 10
Protokół ze sprawdzania zgodności przetwarzania danych
osobowych z przepisami o ochronie danych osobowych

(Data, miejscowość)

1) Oznaczenie administratora danych i adres jego siedziby:

(podać pełną nazwę oraz adres)

2) Imię i nazwisko osoby reprezentującej administratora danych:

3) Wykaz czynności podjętych przez administratora bezpieczeństwa informacji w toku sprawdzenia oraz imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach:

- 4) Datę rozpoczęcia i zakończenia sprawdzenia:

- 5) Określenie przedmiotu i zakresu 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) Wyszczególnienie załączników stanowiących składową część protokołu:

*(Data, miejsce i podpis Administratora Bezpieczeństwa
Informacji)*

