POLITYKA BEZPIECZEŃSTWA
PRZETWARZANIA DANYCH OSOBOWYCH PRZEZ SPÓŁKĘ „WIK" SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ Z SIEDZIBĄ W RYBNIKU

(tekst jednolity obowiązujący od dnia 25 maja 2018 roku)

SŁOWNIK POJĘĆ

1. ADMINISTRATOR DANYCH OSOBOWYCH (ADO/Administrator) – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; w ramach niniejszej Polityki Bezpieczeństwa jest to Spółka „WIK" spółka z ograniczoną odpowiedzialnością z siedzibą w Rybniku (dalej również WIK), ul. Cegielnianej 7, 44-200 Rybnik (adres do korespondencji ul. Cegielniana 7, 44-200 Rybnik), Nr KRS 0000118985, NIP 6411519511, Regon 272923892, adres strony www: http://www.wikrybnik.pl/, adres poczty elektronicznej: biuro@wikrybnik.pl, decydująca o celach i środkach przetwarzania danych osobowych.
2. PRZEDSTAWICIEL - oznacza osobę fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w Unii, która została wyznaczona na piśmie przez administratora lub podmiot przetwarzający do reprezentowania administratora lub podmiotu przetwarzającego, w zakresie ich obowiązków wynikających z rozporządzenia;
3. PODMIOT PRZETWARZAJĄCY - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
4. STRONA TRZECIA - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;
5. DANE OSOBOWE (DANE) - informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Osobą możliwą do zidentyfikowania jest osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
6. DANE GENETYCZNE - oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;
7. DANE BIOMETRYCZNE - oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;
8. DANE DOTYCZĄCE ZDROWIA - oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;
9. ZBIÓR DANYCH – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
10. PRZETWARZANIE DANYCH - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
11. NARUSZENIE OCHRONY DANYCH OSOBOWYCH - oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
12. PROFILOWANIE -oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

13. ZGODA OSOBY, KTÓREJ DANE DOTYCZĄ – dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.
14. ODBIORCA DANYCH –oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;
15. ADMINISTRATOR SYSTEMU INFORMATYCZNEGO – osoba upoważniona przez WIK nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień.
16. OSOBA UPOWAŻNIONA DO PRZETWARZANIA DANYCH OSOBOWYCH – osoba upoważniona przez WIK do przetwarzania danych osobowych
17. UŻYTKOWNIK - osoba upoważniona do przetwarzania danych osobowych w systemie informatycznym, może nim być pracownik WIK, osoba wykonująca pracę na podstawie umowy zlecenia, innej umowy cywilno-prawnej lub innego upoważnienia.
18. BAZA DANYCH OSOBOWYCH - zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci serwera, zewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze rekordów lub obiektów, w których są zapisane dane osobowe.
19. SYSTEM TRADYCYJNY - zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji, wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze.
20. SYSTEM INFORMATYCZNY (SYSTEM) – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
21. IDENTYFIKATOR - ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych systemie informatycznym.
22. HASŁO - ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
23. UWIERZYTELNIENIE - działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
24. ZABEZPIECZENIE DANYCH W SYSTEMIE INFORMATYCZNYM – wdrożenie i eksploatacja stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
25. ROZLICZALNOŚĆ DANYCH - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
26. INTEGRALNOŚĆ DANYCH - właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
27. POUFNOŚĆ DANYCH - właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.
28. RAPORT DANYCH - przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych.
29. USUWANIE DANYCH - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
30. SIEĆ TELEKOMUNIKACYJNA - systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju.
31. TELETRANSMISJA - przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej.
32. SERWER - usługodawca, wyróżniony komputer świadczący usługi na rzecz mających z nim łączność innych komputerów np. przechowujący pliki, pośredniczący w przekazywaniu poczty itp.
33. SIEĆ ROZLEGŁA - sieć publiczną w rozumieniu ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne.
34. FIREWALL - urządzenie lub program, którego głównym zadaniem jest zabezpieczenie sieci wewnętrznej lub komputera przez nieuprawnionym dostępem zewnątrz, jak również zapewnienie kontroli komunikacji na zewnątrz
35. PLIK - ciąg bajtów posiadający swoją nazwę – odróżniającą ją od innych plików – oraz parametry: rozmiar, datę powstania lub datę ostatniej modyfikacji itp.

36. KOPIE ARCHIWALNE - kopie plików danych lub plików oprogramowania tworzone na nośniku wymiennym lub dysku twardym komputera, przeznaczone do ich trwałego przechowywania, jak również do odtworzenia danych w przypadku ich utraty lub uszkodzenia.
37. KOPIE BEZPIECZEŃSTWA - kopie plików danych lub plików oprogramowania tworzone na nośniku wymiennym lub dysku twardym komputera w celu ich odtworzenia w przypadku utraty lub uszkodzenia danych.
38. WIRUS - program, który uaktywniony w pamięci operacyjnej, powoduje wadliwe działanie, zniszczenie lub modyfikację systemu operacyjnego, programu komputerowego lub danych.
39. NOŚNIK KOMPUTEROWY – nośnik służący do zapisu i przechowywania informacji, np. taśmy, dyskietki, płyty CD lub DVD, pendrive-y, dyski twarde.
40. INCYDENT BEZPIECZEŃSTWA – pojedyncze zdarzenie lub seria zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań systemu lub mogą stanowić przyczynę utraty zasobów, reputacji, niezawodności systemów bezpieczeństwa, a także odstępstwa od obowiązujących procedur w zakresie bezpieczeństwa, nawet jeżeli nie prowadzą do wymienionych powyżej skutków.
41. SPRAWDZENIE - czynności audytowe mające na celu zweryfikowanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz podjęcie działań mających na celu doprowadzenie stanu do adekwatnego do wymogów.

§ 1
DEKLARACJA ADMINISTRATORA DANYCH OSOBOWYCH

Administrator Danych Osobowych:

1. deklaruje, że celem spółki WIK jest zapewnienie realizacji jej działalności, przy jednoczesnym zachowaniu najwyższej staranności w zakresie bezpieczeństwa przetwarzanych danych osobowych, dla którego to bezpieczeństwa przykłada najwyższą wagę i zapewnia maksymalny poziom ochrony;
2. stosuje kompleksowe podejście do zagadnień związanych z bezpieczeństwem danych osobowych, w tym stosuje środki i procedury zapewniające wymagany przepisami prawa poziom bezpieczeństwa danych osobowych;
3. deklaruje, że stosowane zasady i reguły postępowania w zakresie bezpieczeństwa danych osobowych, uwzględniają wymagania zawarte w przepisach powszechnie obowiązujących;
4. zobowiązuje każdą osobę upoważnioną do przetwarzania danych osobowych, do zapoznania się z wewnętrznymi dokumentami spółki WIK, dotyczącymi bezpieczeństwa danych osobowych oraz zapoznania się z obowiązującymi w tym zakresie przepisami prawa. Ponadto wymaga od osób upoważnionych do przetwarzania danych osobowych, pisemnego potwierdzenia powyższej okoliczności oraz zobowiązuje do przestrzegania zasad, reguł i postanowień zawartych w wyżej wskazanych dokumentach;
5. deklaruje, że stosowane przez spółkę WIK zasady bezpieczeństwa danych osobowych, będą podlegały ciągłemu doskonaleniu w oparciu o analizy i oceny będące wynikiem merytorycznego przeglądu przestrzegania obowiązujących w powyższym zakresie unormowań. Na podstawie wniosków z takiego przeglądu, będzie dokonywana niezbędna aktualizacja w przypadku zaistnienia zmian w przepisach prawnych, rozwoju technologii, a także zmian organizacyjnych warunkujących dokonanie takiej aktualizacji.

§ 2
CEL POLITYKI BEZPIECZEŃSTWA

1. Polityka bezpieczeństwa opracowana i wdrożona przez spółkę WIK określa podstawy dla procedur wewnętrznych, metod zarządzania i wymagań niezbędnych dla zapewnienia adekwatnych i proporcjonalnych zabezpieczeń, właściwej ochrony informacji i danych administrowanych przez spółkę WIK oraz systemów informatycznych wykorzystywanych do przetwarzania danych, przy uwzględnieniu występującego ryzyka związanego z zagrożeniami, takimi jak: działalność przestępcza, błędy i nieprawidłowości w postępowaniu własnych pracowników, przerwy i zakłócenia w działaniu systemu i naturalne katastrofy.
2. Polityka Bezpieczeństwa została opracowana w celu spełnienia wymogów wynikających z przepisów prawa, w szczególności:
   a) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych inaczej zwane też RODO);
   b) ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych [Dz.U. z 2018 r. poz. 1000];

c) rozporządzenia 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. 2004, nr 100, poz. 1024];
d) rozporządzeniem Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych [Dz.U. 2015, poz. 745].

3. Przepisy prawne, o których mowa w ust. 2, nakładają na Administratora Danych Osobowych następujące obowiązki:
   a) zapewnienie bezpieczeństwa i poufności danych, w tym zabezpieczenie ich przed ujawnieniem,
   b) zabezpieczenie danych przed nieuprawnionym dostępem,
   c) zabezpieczenie danych przed udostępnieniem osobom nieupoważnionym (nieuprawnionym pozyskaniem),
   d) zabezpieczenie przed utratą danych,
   e) zabezpieczenie przed uszkodzeniem lub zniszczeniem danych oraz przed ich nielegalną modyfikacją.
4. Polityka Bezpieczeństwa ma również na celu zapewnienie bezpieczeństwa procesu przetwarzania danych osobowych poprzez identyfikację potencjalnych zagrożeń oraz opracowanie, wdrożenie i stałe monitorowanie funkcjonowania mechanizmów i uregulowań umożliwiających minimalizację i eliminację tych zagrożeń.
5. Celem opracowania i wdrożenia Polityki Bezpieczeństwa jest także poszerzenie wiedzy dotyczącej bezpieczeństwa przetwarzania danych osobowych i świadomości związanych z nim zagadnień.

§ 3
PRZEDMIOT I ZAKRES

1. Mając na uwadze realizację celu, o którym mowa w § 2, spółka WIK podejmuje działania, udokumentowane w Polityce Bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, mające zapewnić optymalny poziom ochrony danych osobowych przetwarzanych przez spółkę WIK.
2. Polityka Bezpieczeństwa została opracowana i jest wdrażana z uwzględnieniem przewidywanych zagrożeń wewnętrznych i zewnętrznych, umożliwiając optymalizację ryzyka w realizacji działalności WIK.
3. Polityka Bezpieczeństwa podlega ciągłemu procesowi oceny w celu jej doskonalenia i aktualizacji. Proces ten oparty jest o działania spółki WIK oraz wnioski wynikające, w szczególności z:
   a) audytów w zakresie bezpieczeństwa oraz weryfikacji stanu ochrony danych osobowych,
   b) nadzoru nad realizacją umów związanych z bezpieczeństwem informacji,
   c) nadzoru nad urządzeniami i systemami zabezpieczeń technicznych,
   d) nadzoru nad zabezpieczeniem funkcjonowania systemów teleinformatycznych,
   e) realizacji kontroli dostępu do aplikacji systemowych,
   f) analizowania kierunków zmian i tendencji rozwoju techniki i technologii oraz metod działania zabezpieczeń,
   g) analizowania zmieniającej się w czasie hierarchii zagrożeń.
4. Polityka Bezpieczeństwa jest dokumentem podrzędnym w stosunku do obowiązujących przepisów prawa, uwzględnia wymagania wynikające z nich i musi zostać do nich dostosowana w przypadku stwierdzenia jakichkolwiek niezgodności z obowiązującym stanem prawnym.
5. Przedmiotem Polityki Bezpieczeństwa jest określenie zastosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych osobowych objętych ochroną, a w szczególności zabezpieczeń danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Podczas wyboru zabezpieczeń należy uwzględniać koszty ich wdrożenia w odniesieniu do ryzyka oraz potencjalnych strat (również aspektów niematerialnych np. utraty reputacji), które mogą być skutkiem naruszenia stanu ochrony danych osobowych.
6. Polityka Bezpieczeństwa ochrony danych osobowych obowiązuje przy przetwarzaniu danych będących własnością lub jedynie administrowanych przez spółkę WIK w całym zakresie ich przetwarzania, tj. w formie tradycyjnej oraz elektronicznej z uwagi na fakt, iż jedynie kompleksowe podejście do zagadnienia ochrony

informacji gwarantuje skuteczność podejmowanych działań. Dane osobowe korzystają z ochrony już wówczas, gdy mogą się znaleźć w bazie danych.

7. W przypadku, gdy przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych osobowych, przewidują dalej idącą ochronę, wówczas stosuje się te przepisy w pierwszej kolejności.
8. W przypadku powierzenia przez Administratora Danych Osobowych przetwarzania danych osobowych, podmioty którym te dane powierzono są obowiązane prowadzić własną dokumentację wymaganą przez właściwe przepisy prawa.
9. Polityka Bezpieczeństwa ochrony danych osobowych ma zastosowanie w stosunku do wszystkich pracowników spółki WIK, konsultantów, stażystów, praktykantów, osób realizujących zadania w oparciu o umowy cywilnoprawne i innych osób mających dostęp do danych osobowych podlegających ochronie, jak również osób i podmiotów, z którymi zostały zawarte umowy współpracy lub które na innych podstawach współpracują ze spółką WIK.
10. Dane osobowe są chronione zgodnie z obowiązującymi przepisami prawa dotyczącymi bezpieczeństwa i poufności przetwarzanych danych. Systemy informatyczne oraz tradycyjne, które przechowują dane osobowe, są chronione odpowiednimi środkami technicznymi. Opracowane procedury określają obowiązki użytkownika zbiorów tradycyjnych oraz zasady korzystania z systemów informatycznych.

§ 4
PODMIOTY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH – PRAWA I OBOWIĄZKI

1. Administratorem Danych Osobowych wskazanych w niniejszym dokumencie, jest WIK spółka z ograniczoną odpowiedzialnością. Spółka WIK może wyznaczyć przedstawiciela (pełnomocnika) ds. ochrony danych osobowych, który będzie w imieniu administratora, bezpośrednio realizował i wykonywał obowiązki administratora w zakresie ochrony przetwarzanych danych osobowych, ze szczególnym uwzględnieniem obowiązku szacowania ryzyka oraz monitorowania i reagowania na wszelkie incydenty naruszenia ochrony danych osobowych.
2. Spółka WIK jako Administrator Danych Osobowych odpowiedzialna jest za organizację właściwego zabezpieczenia danych, wdrożenie przepisów prawa oraz unormowań niniejszej Polityki Bezpieczeństwa, a także podejmowanie decyzji i wszelkich działań mających na celu zapewnienie zgodności przetwarzania danych z obowiązującymi przepisami nadrzędnymi i unormowaniami wewnętrznymi. Powyższe zadania realizowane są w oparciu o decyzje właściwych organów, które ponoszą prawną odpowiedzialność za stan bezpieczeństwa danych osobowych.
3. Wydawcą Polityki Bezpieczeństwa ochrony danych osobowych odpowiedzialnym za jej adekwatność do przepisów prawnych i uprawnionym do jej modyfikacji jest zarząd spółki WIK.
4. Administrator Danych Osobowych powołuje Inspektora ochrony danych osobowych w sytuacjach prawem przewidzianych, lub w innych sytuacjach gdy tak zdecyduje.
5. Inspektor ochrony danych jest odpowiedzialny za:
   a. zapewnienie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:
      i. sprawdzenie zgodności przetwarzania danych osobowych;
      ii. nadzorowanie opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednie do kategorii danych objętych ochroną oraz przestrzegania zasad z niej określonych;
      iii. zapewnienie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;
   b. prowadzenie rejestrów i ewidencji wymaganych przez przepisy prawa;
   c. monitoruje zdarzenia i naruszenia ochrony danych osobowych;
   d. stanowi głos doradczy i opiniotwórczy dla ADO;
   e. dokonuje cyklicznej weryfikacji, monitorowania i aktualizacji procedur i zasad przetwarzania danych osobowych.
6. Inspektorem ochrony danych może być osoba, która:
   a) ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych
   b) posiada odpowiednią wiedzę w zakresie ochrony danych,
7. Inspektorem ochrony danych nie może być członek Zarządu spółki WIK.
8. Inspektor ochrony danych realizuje kontrole zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych dokonując sprawdzeń wybranych obszarów działalności ADO:

a) planowych – według wcześniej przygotowanego przez siebie planu, musi uwzględniać w szczególności zbiory danych osobowych i systemy informatyczne służące do przetwarzania danych osobowych oraz konieczność weryfikacji zgodności przetwarzania danych osobowych z przepisami prawa. Plan sprawdzeń obejmuje co najmniej jedno sprawdzenie i obejmuje okres nie dłuższy niż rok, przy czym zbiory danych osobowych oraz systemy informatyczne służące do przetwarzania lub zabezpieczania danych powinny być objęte sprawdzeniem co najmniej raz na 5 lat.
b) doraźnych – wykonywane w przypadku powzięcia informacji lub nawet uzasadnionego podejrzenia o naruszeniu ochrony danych. Są one niezależne od sprawdzeń planowych, podejmowane niezwłocznie, po uprzednim powiadomieniu ADO o rozpoczęciu sprawdzenia doraźnego,
c) na zlecenie organu nadzorczego - w przypadku zwrócenia się przez organ o wykonanie kontroli.

9. ADO może powierzyć Inspektorowi wykonywanie innych obowiązków, jeżeli nie naruszy to prawidłowego wykonywania zadań Inspektora ochrony danych.
10. Z przeprowadzonych czynności sprawdzających Inspektor sporządza sprawozdanie, w terminie do 7 dni.
11. Administrator Danych Osobowych może wyznaczyć Administratora Systemu Informatycznego, który:
    a) wykonuje wszystkie prace niezbędne do efektywnego oraz bezpiecznego zarządzania systemem informatycznym;
    b) zapewnienia ciągłość i bezpieczeństwo funkcjonowania systemu informatycznego, w szczególności nadaje oraz odbiera uprawnienia w imieniu ADO do poszczególnych aplikacji, programów, systemów operacyjnych lub urządzeń elektronicznych;
    c) jest zobowiązany do wdrożenia wymogów wynikających w przepisów prawa oraz Polityki Bezpieczeństwa ochrony danych osobowych, oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych w zakresie ochrony danych osobowych;
    d) zapewnia, poprzez zastosowanie odpowiednich środków i metod kontroli dostępu, że wyłącznie autoryzowany personel ma dostęp do systemów informatycznych;
    e) przydziela użytkownikom systemu informatycznego konta i hasła;
    f) ewidencjonuje użytkowników systemu;
    g) zapewnia dopuszczenie do zakupu i modernizacji oprogramowania na potrzeby spółki WIK z zachowaniem wymogów przewidzianych dla systemów przetwarzających dane osobowe, w tym opiniowanie możliwości wykorzystania systemów informatycznych i środków komunikacji pod kątem bezpieczeństwa informatycznego;
    h) zapewnia nadzór nad naprawami i likwidacją urządzeń komputerowych, na których zapisane są dane osobowe;
    i) zapewnia nadzór nad przeglądami, konserwacją, uaktualnieniem systemów informatycznych służących do przetwarzania danych osobowych;
    j) zapewnia bezpieczną wymianę danych w sieci wewnętrznej i bezpieczne przesyłanie danych za pośrednictwem urządzeń teletransmisji;
    k) podejmuje działania zabezpieczające w sytuacji stwierdzenia naruszenia zabezpieczeń systemów informatycznych, w których są przetwarzane dane osobowe, w tym przesyłane drogą teletransmisji;
    l) nadzoruje wykonywanie kopii zapasowych, ich przechowywanie oraz okresowe sprawdzanie pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu informatycznego;
    m) przeprowadza inwentaryzację zasobów informatycznych
    n) zabezpiecza informacje niezbędnych do stwierdzenia naruszenia ochrony danych osobowych związanego z systemem informatycznym.
12. Spółka WIK nie powołała Administratora Systemu Informatycznego.
13. Zarząd spółki WIK odpowiada za:
    a. wdrożenie i realizację obowiązujących w spółce WIK przepisów i aktów prawnych wewnętrznych z zakresu ochrony danych osobowych,
    b. stosowanie przez podległych pracowników i współpracowników, środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, zgodnie z wymogami wynikającymi z obowiązujących aktów prawnych wewnętrznych,
    c. zarządzanie – w zakresie przyznanych kompetencji - systemem przetwarzania danych osobowych, w tym nadzór nad bazami danych oraz obiegiem i przechowywaniem nośników zawierających dane osobowe,

d. wdrożenie niezbędnych wymogów i zarządzanie bazami danych osobowych pozyskanymi w ramach umów powierzenia przetwarzania danych osobowych, np. w przypadku realizacji projektów zewnętrznych,
e. odbycie przez upoważnione osoby szkoleń z zakresu ochrony danych osobowych oraz pobranie od nich potwierdzeń znajomości przepisów i aktów prawnych wewnętrznych z przedmiotowego zakresu,
f. rozpoczynanie i podejmowanie przedsięwzięć mających na celu doskonalenie ochrony danych osobowych,
g. podejmowanie, stosownie do zaistniałej sytuacji i unormowań, niezbędnych działań w przypadku naruszenia lub uzasadnionego podejrzenia naruszenia zasad ochrony danych osobowych,
h. dopuszczanie do przetwarzania danych osobowych wyłącznie pracowników lub inne osoby do tego upoważnione i zapewnienie adekwatności posiadanych przez nich dostępów do danych i urządzeń, do rzeczywistych potrzeb na stanowisku pracy lub wykonywanych zadań,
i. udostępnianie, zgodnie z obowiązującymi przepisami prawa i unormowaniami wewnętrznymi, danych osobowych podmiotom spoza spółki WIK oraz prowadzenie ewidencji udostępniania tychże danych osobowych,

14. Każdy pracownik spółki WIK oraz inne osoby upoważnione przez spółkę WIK do przetwarzania danych osobowych, ponoszą bezpośrednią odpowiedzialność za stan bezpieczeństwa przetwarzanych danych osobowych, mają również obowiązek współpracy z osobami odpowiedzialnymi za realizację zadań wynikających z Polityki Bezpieczeństwa. W szczególności osoby te odpowiedzialne są za:
    a) zapoznanie się z unormowaniami dotyczącymi ochrony danych osobowych oraz aktami prawnymi wewnętrznymi z przedmiotowego zakresu;
    b) podpisanie oświadczenia potwierdzającego znajomości przepisów i aktów prawnych wewnętrznych z zakresu ochrony danych osobowych własnoręcznym podpisem;
    c) udział w szkoleniach z zakresu ochrony danych;
    d) stały nadzór oraz dbałość o bezpieczeństwo danych osobowych, do których ma dostęp, przetwarzanych zarówno w postaci tradycyjnej, jak i w systemie informatycznym, w szczególności utrzymanie właściwego poziomu bezpieczeństwa w zakresie swoich obowiązków i przyznanych uprawnień;
    e) podjęcie, przewidzianych przepisami i aktami prawnymi wewnętrznymi, środków mających na celu właściwe zabezpieczenie danych;
    f) wykorzystanie danych i ich przesyłanie wyłącznie w ramach realizowanych czynności, zgodnie z obowiązującymi wymogami;
    g) zachowanie w tajemnicy danych osobowych, pozyskanych w trakcie trwania i po ustaniu współpracy;
    h) postępowanie zgodnie z przyjętymi zasadami i minimalizacja zagrożeń wynikających z ludzkich błędów.
15. Zasady odpowiedzialności, uregulowane są w obowiązujących przepisach prawnych, w szczególności Kodeksie Pracy, Kodeksie Karnym, Kodeksie Cywilnym.

§ 5
PROCEDURY – ZASADY OGÓLNE

1. Nadrzędną zasadą jest ochrona danych przed nieautoryzowanym dostępem, ujawnieniem, powieleniem, modyfikacją, zniszczeniem, utratą, zatajeniem, nieprawidłowym wykorzystaniem lub kradzieżą.
2. Poza ochroną danych będących własnością Administratora danych osobowych ochronie podlegają dane stanowiące własność osób trzecich, o ile zostały przekazane na zasadzie wzajemnego zaufania i mają charakter informacji chronionych.
3. Wprowadzone rozwiązania organizacyjne mają na celu zapewnienie efektywności działań.
4. Uwzględniając powszechnie obowiązujące zasady bezpieczeństwa, w zależności od specyfiki pojawiających się zagrożeń spółka WIK definiuje własne wymagania w tym zakresie, określając je w:
    a) uchwałach Zarządu,
    b) zawieranych umowach,
    c) innych dokumentach.
5. W celu utrzymania wysokiego poziomu bezpieczeństwa spółka WIK współpracuje z kontrahentami zewnętrznymi, jak również korzysta z usług sprawdzonych podmiotów i osób, posiadających najlepsze rekomendacje i gwarantujących najwyższy poziom, których dobór prowadzony jest zgodnie z obowiązującymi przepisami prawa.

6. Przyjęte zasady bezpieczeństwa danych i ich przetwarzania, tworzą podstawy dla wprowadzenia mechanizmów zarządzania, procedur i niezbędnych wymagań dla zapewnienia ochrony wszelkich przetwarzanych danych, niezależnie od systemów, sposobów i miejsc przetwarzania.
7. Realizacja Polityki Bezpieczeństwa ochrony danych osobowych wymaga nie tylko przestrzegania, określonych w poszczególnych regulacjach wchodzących w jego skład, zasad bezpieczeństwa, ale przede wszystkim bieżącego analizowania zagrożeń i korygowania istniejących rozwiązań oraz prognozowania przewidywanych kierunków powstawania zagrożeń, a także doskonalenia form i metod przeciwdziałania naruszeniom zasad bezpieczeństwa oraz przestępczości.
8. Przetwarzanie danych osobowych może mieć miejsce, gdy:
   a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów. Zapytanie o zgodę musi być wyraźne, szczegółowe, w zrozumiałej i łatwo dostępnej formie oraz w jasnym i prostym języku.
   b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
   c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
   d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby;
   e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
   f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem (podstawa nie dotyczy organów publicznych).
9. W sytuacji, gdy przesłanką legalnego przetwarzania danych osobowych jest zgoda osoby, której dane dotyczą warunkiem jej skuteczności jest dobrowolność oraz świadomość jej złożenia.
10. Szczegółowe zasady dotyczące warunków legalnego przetwarzania danych osobowych oraz praw i obowiązków związanych z ich przetwarzaniem zarówno administratora danych, jak i osoby, której dane dotyczą, w szczególności prawa do dobrowolnego podania danych osobowych, ich modyfikacji oraz sprzeciwu wobec ich przetwarzania określa RODO.

§ 6
PROCEDURY SZCZEGÓŁOWE PRZETWARZANIA DANYCH OSOBOWYCH

1. Spółka WIK zbierając dane osobowe od osoby, której dane dotyczą, wskazuje w klauzuli informacyjnej następujące dane:
   a) pełna nazwa i adres siedziby (tożsamość i dane kontaktowe) administratora,
   b) dane kontaktowe inspektora ochrony danych - jeżeli został wyznaczony,
   c) cele przetwarzania danych osobowych oraz podstawę prawną,
   d) opis prawnie uzasadnionego interesu – jeżeli na tej podstawie przetwarza się dane,
   e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją,
   f) informację o zamiarze przekazania danych do państwa trzeciego,
   g) okres przechowywania danych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
   h) informacja o prawie dostępu do danych, sprostowania, usunięcia, ograniczenia przetwarzania, prawie wniesienia sprzeciwu i przenoszeniu danych, prawie do cofnięcia zgody, wniesienia skargi,
   i) informacja czy podanie danych jest wymogiem ustawowym, umownym, warunkiem zawarcia umowy, podanie konsekwencji niewskazania danych,
   j) informacja o zautomatyzowanym podejmowaniu decyzji, profilowaniu (podanie zasad i konsekwencji).
2. Obowiązek informacyjny wypełniany jest w chwili zbierania danych. Nie ma znaczenia sposób zbierania danych: pisemny, telefoniczny, czy też w kontaktach bezpośrednich.
3. W przypadku zbierania danych nie od osoby, której one dotyczą, administrator obowiązany jest poinformować tę osobę dodatkowo o źródle, z którego pozyskane są dane oraz o kategorii danych.
4. Obowiązku informacyjnego nie wypełnia się jeśli:
   a) przepis innej ustawy zezwala na przetwarzanie danych bez ujawnienia faktycznego celu ich zbierania,
   b) osoba, której dane dotyczą, posiada przedmiotowe informacje.

5. Spółka WIK jako Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi w drodze umowy powierzenia przetwarzania danych osobowych.
6. Do umów zawieranych z podmiotami zewnętrznymi, przy realizacji których istnieje prawdopodobieństwo dostępu do pomieszczeń lub informacji i danych podlegających ochronie powinny zostać włączone klauzule:
   a) dotyczące obowiązku ochrony tych informacji przez strony umowy zarówno w trakcie trwania umowy, jak i po jej ustaniu,
   b) ograniczenia dostępu do informacji wyłącznie do osób związanych z realizacją umowy,
   c) zakazu ujawniania danych,
   d) odpowiedzialności w przypadku naruszenia bezpieczeństwa danych zarówno przez podmiot jak i zatrudnionych pracowników, a w przypadku umów powierzenia przetwarzania danych osobowych również klauzule określające:
      i. przedmiot i czas przetwarzania,
      ii. charakter i cel oraz zakres powierzenia przetwarzania danych osobowych,
      iii. rodzaj danych osobowych oraz kategorie osób, których dane dotyczą,
      iv. obowiązki i prawa administratora,
      v. zasady przetwarzania i ochrony danych zgodnie z obowiązującymi przepisami,
      vi. spełnienie wymogów wynikających z przepisów,
      vii. prawo kontroli spełnienia wymogów podmiotu, któremu powierzono dane zarówno przed zawarciem umowy, jak i w trakcie jej trwania,
      viii. odpowiedzialność podmiotu i jego pracowników z tytułu powierzenia przetwarzania danych,
      ix. obowiązek poinformowania o wszelkich naruszeniach w zakresie przetwarzania danych osobowych oraz kontrolach uprawnionych instytucji zewnętrznych oraz o wszelkich innych okolicznościach istotnych z punktu widzenia przetwarzania danych,
      x. skutki naruszenia zasad przetwarzania danych osobowych,
      xi. obowiązek podjęcia działań mających na celu zapobiegnięcie wyciekowi danych oraz wdrożenie środków zapobiegawczych mających na celu brak możliwości wystąpienia naruszeń w przyszłości,
      xii. obowiązek świadczenia pomocy administratorowi poprzez odpowiednie środki techniczne i organizacyjne, aby mógł on wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą;
      xiii. obowiązek zwrotu lub usunięcia danych po zakończeniu świadczenia usług związanych z przetwarzaniem, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;
      xiv. prawo do natychmiastowego rozwiązania umowy w przypadku braku przestrzegania jej postanowień.
7. Podmiot, któremu powierzono przetwarzanie danych osobowych może przetwarzać te dane wyłącznie w zakresie i celu przewidzianym w umowie, ponosi również odpowiedzialność za zachowanie wszelkich wymogów wynikających z przepisów prawa w zakresie ochrony danych osobowych, w szczególności zastosowanie wymogów technicznych i organizacyjnych do zabezpieczenia przedmiotowych danych.
8. Dane osobowe administrowane przez spółkę WIK mogą być udostępniane wyłącznie na podstawie obowiązujących przepisów prawa.
9. Każdej osobie, której dane są przetwarzane, przysługuje prawo do kontroli przetwarzania tych danych, a w szczególności prawo wglądu do treści danych osobowych oraz:
   a) Prawo do informacji o:
      i. fakcie przetwarzania danych jej dotyczących (czy istnieje zbiór danych),
      ii. pełnej nazwie i adresie siedziby Administratora Danych Osobowych,
      iii. celu przetwarzania danych,
      iv. zakresie wykorzystywanych danych (kategoriach przetwarzanych informacji),
      v. sposobie przetwarzania danych (środkach, przy pomocy których dane są przetwarzane),
      vi. dacie, od kiedy dane są przetwarzane przez Administratora Danych Osobowych (dacie włączenia do zbioru),
      vii. źródle danych, chyba że Administrator Danych Osobowych zobowiązany jest do zachowania w tym zakresie tajemnicy,
      viii. sposobie udostępniania danych oraz odbiorcach lub kategoriach odbiorców, którym dane są udostępniane,

ix. przesłankach podjęcia rozstrzygnięcia podjętego podczas zawierania lub wykonywania umowy uwzględniającego wniosek osoby, której dane dotyczą;

b) prawo do żądania uzupełnienia, uaktualnienia, sprostowania, czasowego lub stałego wstrzymania przetwarzania danych lub ich usunięcia;

c) prawo do wniesienia żądania zaprzestania przetwarzania danych oraz sprzeciwu wobec przetwarzania danych, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych,

d) prawo do przenoszenia danych.

10. Udostępnienie informacji, o których mowa w pkt. 1 odbywa się na wniosek zainteresowanej osoby. Fakt udostępnienia informacji należy odnotować w systemie, w którym przetwarzane są dane podlegające udostępnieniu, a w przypadku braku takiej możliwości w ewidencji udostępniania danych osobowych.
11. Administrator Danych Osobowych na wniosek, zobowiązany jest, poinformować zainteresowaną osobę o przysługujących jej prawach oraz udzielić informacji, o których udostępnienie zainteresowana osoba wnioskuje.
12. Jeżeli Administrator Danych Osobowych poweźmie wątpliwości co do tożsamości osoby korzystającej z któregokolwiek prawa określonego w pkt. 9, ma on prawo zweryfikować jej tożsamość poprzez zadanie pytania kontrolnego, na które odpowiedź powinna posiadać tylko ta osoba lub ustalić jej tożsamość w inny sposób.
13. Uzupełnienie, uaktualnienie, sprostowanie, czasowe lub stałe wstrzymanie przetwarzania danych osobowych następuje, na wniosek zainteresowanej osoby, gdy dane są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane niezgodnie z obowiązującymi przepisami.
14. Po złożeniu przez zainteresowaną osobę wniosku, o którym mowa w pkt. 4, Administrator Danych Osobowych zobowiązany jest bezzwłocznie do dokonania stosownych czynności w celu uzupełnienia, uaktualnienia, sprostowania, czasowego lub stałego wstrzymania przetwarzania jej danych, chyba że do odmiennego postępowania uprawniają go obowiązujące przepisy prawa.
15. Do przesyłania dokumentów elektronicznych z danymi osobowymi należy stosować systemy informatyczne gwarantujące bezpieczeństwo przesyłanych danych, tj. strony szyfrowane, indywidualne katalogi wymiany.
16. Systemy informatyczne służące do przesyłania danych oraz generowania plików przeznaczonych do wysłania powinny posiadać uaktywnione mechanizmy kontroli dostępu w postaci loginu i hasła.
17. Dane osobowe należy przesyłać w formie niejawnej i umożliwiającej ich uwierzytelnienie, np. poprzez spakowanie z hasłem lub szyfrowane kanały.
18. W przypadku, gdy elektroniczne przesyłanie danych osobowych, do podmiotów zewnętrznych uprawnionych do ich otrzymania na mocy przepisów prawa, stanowi udostępnianie tych danych, należy przedmiotowy fakt odnotować w systemie lub zaewidencjonować w Ewidencji udostępniania danych osobowych.

§ 7
FORMA I OBSZAR PRZETWARZANIA DANYCH OSOBOWYCH

1. Dane osobowe w spółce WIK, w zależności od rodzaju danych są gromadzone, przechowywane, edytowane, archiwizowane w kartotekach, skorowidzach, księgach, wykazach, zestawieniach oraz innych zestawach i zbiorach ewidencyjnych, mających postać dokumentów papierowych, jak również w systemach informatycznych na elektronicznych nośnikach informacji.
2. Podstawowym miejscem przetwarzania danych osobowych jest siedziba spółki WIK, zlokalizowana pod adresem Rybnik, ul. Cegielniana 7.
3. Z uwagi jednak na rodzaj działalności prowadzonej przez spółkę WIK, każdorazowe miejsce prowadzenia działalności spółki WIK stanowi obszar przetwarzania danych osobowych. W szczególności dotyczy to miejsca podejmowania czynności i działalności prowadzonej przez członków władz spółki WIK.
4. Administrator prowadzi:
    a) Rejestr Czynności przetwarzania danych osobowych;
    b) Wykaz obszaru przetwarzania danych osobowych;
    c) Inwentaryzację zasobów informatycznych (IT);
    d) Ewidencję umów powierzenia przetwarzania danych osobowych;
    e) Ewidencję osób upoważnionych do przetwarzania danych osobowych;
    f) Rejestr Naruszeń Bezpieczeństwa ochrony danych osobowych;
    g) Rejestr zgód na przetwarzanie danych.

§ 8
OPIS KATEGORII DANYCH OSOBOWYCH ORAZ SPOSOBU PRZEPŁYWU DANYCH

1. Kategorie przetwarzanych danych osobowych podzielone są funkcjonalnie ze względu na cel danej kategorii. Przetwarza się je, w tym gromadzi i przechowuje zarówno na nośnikach papierowych, jak i w systemie informatycznym.
2. Ze względu na rodzaj i charakter danych osobowych zawartych w zbiorach wyróżnia się dwie kategorie danych:
    a. dane osobowe zwykłe,
    b. dane osobowe sensytywne.
5. W przypadku przetwarzania danych osobowych w postaci papierowej odbywa się ono przy wykorzystaniu wszelkiego typu druków, formularzy, kartotek, ksiąg, akt, albumów oraz innej dokumentacji gromadzonej w spółce WIK.
6. W przypadku przetwarzania danych osobowych w postaci elektronicznej odbywa się ono przy użyciu systemów informatycznych wykorzystywanych przez Administratora. Pliki bazodanowe przechowywane są na dedykowanych serwerach. Szczegółowy opis struktury danych osobowych przetwarzanych w postaci elektronicznej, relacji pomiędzy danymi oraz procesy przetwarzania danych zawarte są w dokumentacji technicznej systemów informatycznych wykorzystywanych do przetwarzania przedmiotowych danych oraz w prowadzonych wykazach, ewidencjach i rejestrach.

§ 9
ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DO ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANIA DANYCH

1. Przetwarzania danych osobowych należy dokonywać w warunkach zabezpieczających te dane przed osobami nieupoważnionymi.
2. Pomieszczenia, w których przetwarzane są dane osobowe zabezpieczone są na czas nieobecności osób upoważnionych do przetwarzania danych osobowych, w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, tj. poprzez zabezpieczenia techniczne, fizyczne i ochronę fizyczną budynku i pomieszczeń.
3. Uzasadnione względami służbowymi przebywanie w tych pomieszczeniach osób nieuprawnionych do dostępu do danych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych oraz w warunkach zapewniających bezpieczeństwo tych danych.
4. Osoby upoważnione do przetwarzania danych osobowych obowiązane są do prawidłowego zabezpieczania urządzeń i danych na swoich stanowiskach pracy.
5. Dostęp do kluczy do pomieszczeń stanowiących obszar przetwarzania danych osobowych posiadają wyłącznie osoby uprawnione przez administratora do wstępu do tych pomieszczeń.
6. Wszelkie urządzenia i nośniki zawierające dane osobowe, takie jak serwery, komputery, urządzenia teletransmisyjne, szafy zawierające kopie danych muszą znajdować się w pomieszczeniach lub warunkach, uniemożliwiających dostęp do nich osób nieupoważnionych.
7. Wyłączniki oraz zabezpieczenia zasilania elektrycznego, w już użytkowanych obiektach, są zabezpieczone przed dostępem osób nieupoważnionych.
8. Dostęp do pomieszczeń, w których odbywa się przetwarzanie danych osobowych winien być ściśle kontrolowany poprzez stosowane zabezpieczenia organizacyjne i mechaniczne oraz zainstalowane systemy alarmowe.
9. Za bezpieczeństwo danych osobowych zapisanych w formie papierowej odpowiedzialne są osoby je przetwarzające.
10. Wszystkie dane osobowe przetwarzane w formie papierowej, powinny być zabezpieczone przed osobami nieupoważnionymi oraz przechowywane w urządzeniach gwarantujących dostęp do nich wyłącznie osób uprawnionych tj. przynajmniej w pomieszczeniach zamykanych na klucz zabezpieczonych monitorowanym systemem alarmowym, z zastosowaniem dodatkowego zabezpieczenia w postaci szafy drewnianej zamykanej na klucz lub zamykanej na klucz szafy metalowej – w odniesieniu do szczególnie istotnych i wrażliwych danych.
11. Wszelkie dokumenty i wydruki zawierające dane osobowe przeznaczone do usunięcia należy niszczyć w stopniu uniemożliwiającym ich odczytanie (przy użyciu niszczarki). Dopuszcza się możliwość niszczenia dokumentów zawierających dane osobowe przez specjalistyczne firmy zewnętrzne. Warunkiem skorzystania z usług tego typu firm jest zawarcie umowy cywilnoprawnej, w której należy zawrzeć klauzule zobowiązujące

firmę do zapewnienia stanu poufności informacji uzyskanych w toku realizacji umowy oraz określić kwestie związane z przekazaniem dokumentów do zniszczenia, sposobem zniszczenia oraz potwierdzenia tego faktu w postaci protokołów i certyfikatów.

12. System informatyczny służący do przetwarzania danych osobowych zabezpiecza się w szczególności przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu oraz przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
13. System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.
14. W przypadku zastosowania zabezpieczeń logicznych obejmują one:
    a) kontrolę przepływu informacji pomiędzy systemem informatycznym wykorzystywanym przez Administratora a siecią publiczną,
    b) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego w spółce WIK.
15. Telefony komórkowe wykorzystywane przez Administratora powinny zostać zabezpieczone w szczególności poprzez zastosowanie hasła dostępu w celu uzyskania wglądu na ekran telefonu lub innych rodzajów zabezpieczeń na które pozwala wykorzystywana przez telefon technologia.
16. Jeżeli telefon komórkowy wykorzystywany jest przez Administratora jest używany jest również w celu dostępu do poczty elektronicznej Administratora lub innych systemów komputerowych, telefon taki powinien zostać zabezpieczony w szczególności poprzez zainstalowanie oprogramowania antywirusowego.
17. Administrator Danych Osobowych obowiązany jest do zabezpieczenia wykorzystywanych do przetwarzania danych osobowych urządzeń, dysków lub innych elektronicznych nośników informacji. Uregulowania określające rodzaj zastosowanych zabezpieczeń nośników znajdują się w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych.
18. System informatyczny służący do przetwarzania danych osobowych – z wyjątkiem systemu służącego do przetwarzania danych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie – powinien zapewniać, aby możliwe było w tym systemie odnotowanie:
    a) daty pierwszego wprowadzenia danych osobowych do systemu oraz odnotowanie identyfikatora użytkownika wprowadzającego dane do systemu – powyższy obowiązek nie dotyczy systemu informatycznego, do którego dostęp posiada wyłącznie jedna osoba. W/w odnotowania następują automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych,
    b) źródła danych w przypadku zbierania danych nie od osoby, której dane dotyczą,
    c) informacji o odbiorcach, którym dane zostały udostępnione, dacie i zakresie ich udostępnienia,
    d) wniesienia sprzeciwu osoby wobec przetwarzania jej danych osobowych: w celach marketingowych lub przekazywania danych innemu administratorowi danych,
    e) sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa powyżej.
19. W przypadku wykorzystywania do przetwarzania danych osobowych komputerów przenośnych lub telefonów służbowych ich użytkownik zobowiązany jest do zachowania szczególnej ostrożności podczas transportu, przechowywania i używania poza wyznaczonym przez ADO obszarem przetwarzania danych osobowych, w tym stosowania środków ochrony kryptograficznej wobec przetwarzanych danych. Użytkownik komputera przenośnego lub telefonu służbowego odpowiada za powierzone mu urządzenie oraz wszelkie operacje wykonywane przy jego użyciu.
20. Komputery przenośne oraz telefony służbowe, wykorzystywane do przetwarzania danych osobowych, po zakończonej pracy, winny być przechowywane w warunkach zapewniających ich bezpieczeństwo. Za właściwe zabezpieczenie przedmiotowych urządzeń odpowiedzialni są ich użytkownicy.
21. Lokalizacja urządzeń komputerowych (komputerów typu PC, terminali, drukarek) oraz telefonów powinna uniemożliwiać dostęp do nich osób nieuprawnionych oraz wgląd do danych wyświetlanych na monitorach komputerowych lub na ekranie telefonu.
22. W przypadku oddalenia się użytkownika od stanowiska pracy, należy pozostawić system w takim stanie, aby osoby nieupoważnione nie miały do niego dostępu. W tym celu konieczne jest zablokowanie komputera (jeżeli istnieją takie możliwości techniczne) oraz stosowanie chronionych hasłem wygaszaczy ekranu z odpowiednim (tj. nie dłuższym niż 10 minut) czasem nieaktywności do ich uruchomienia.
23. Wszystkie prace remontowe, konserwacyjne, naprawcze, a także porządkowe odbywają się w oparciu o zawarte umowy.

24. W przypadku naprawy sprzętu komputerowego lub telefonu komórkowego dane należy zabezpieczyć, natomiast w przypadku naprawy sprzętu poza obszarem przetwarzania danych osobowych, po zabezpieczeniu danych – należy je trwale usunąć z dysku. Gdy nie ma możliwości usunięcia danych naprawa powinna być nadzorowana przez osobę upoważnioną przez administratora.
25. Szczególnemu nadzorowi podlegają urządzenia umożliwiające tworzenie i przenoszenie dużych ilości danych, w tym nagrywarki DVD oraz nośniki typu pendrive, a także nośniki komputerowe zawierające dane osobowe. Do ich ochrony i zabezpieczenia zobowiązani są wszyscy ich użytkownicy.
26. W przypadku uszkodzenia nośników komputerowych, o których mowa w pkt 23, użytkownicy zobowiązani są do ich zniszczenia lub przekazania do właściwych służb informatycznych w celu zniszczenia.
27. Uszkodzone nośniki komputerowe (w tym dyski twarde), zawierające dane osobowe, powinny być fizycznie niszczone w sposób uniemożliwiający dostęp do danych osób niepowołanych. Do czasu zniszczenia nośniki komputerowe powinny być zabezpieczone przed dostępem osób nieupoważnionych.
28. Dopuszcza się ponowne wykorzystanie urządzeń i nośników komputerowych zawierających dane osobowe.
29. Urządzenia i nośniki komputerowe zawierające dane osobowe, przeznaczone do ponownego wykorzystania lub przekazania innemu podmiotowi należy - przed ich wykorzystaniem lub przekazaniem - pozbawić zapisu w sposób gwarantujący trwałe usunięcie danych (za pomocą specjalistycznego oprogramowania).
30. System informatyczny musi zapewniać autoryzację i rozliczalność operacji. Każde działanie w systemie informatycznym powinno być jednoznacznie przypisane do unikalnego identyfikatora.
31. Dostęp do danych w systemie informatycznym powinien być kontrolowany. Jest on możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia. Identyfikator przydzielany jest użytkownikowi na stałe. Uwierzytelnienie użytkownika następuje za pomocą indywidualnego hasła. Szczegółowe zasady w zakresie metod i środków uwierzytelniania oraz sposobu zarządzania hasłami do systemów informatycznych i wymagań dotyczących haseł określone są w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych.
32. Dostęp do nagrań z kamery monitoringu zainstalowanej w siedzibie Administratora posiada wyłącznie Administrator.
33. Nagrania o których mowa w ust. 32 przechowywane są na komputerze do którego dostęp ma wyłącznie Administrator oraz zabezpieczone hasłem.
34. W celu ochrony danych osobowych przetwarzanych w systemach informatycznych przed szkodliwym oprogramowaniem należy stosować zabezpieczenia techniczne minimalizujące ryzyko utraty lub uszkodzenia danych.
35. Sposób postępowania i ochrony zasobów informatycznych przed wirusami normuje Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych.
36. W zakresie zapewnienia poufności danych osobowych, administrator stosuje ponadto następujące środki techniczne i organizacyjne:
    a) Dostęp do środków teletransmisji oraz poufnych danych osobowych zabezpieczono za pomocą mechanizmów uwierzytelnienia zaprogramowanych w języku PHP.
    b) Mechanizmy uwierzytelniające wykorzystują dedykowane konta użytkowników zabezpieczone hasłem.
    c) Dostęp do środków teletransmisji oraz poufnych danych osobowych możliwy jest jedynie z dedykowanego konta Administratora Danych Osobowych.
    d) Hasła wprowadzane przez użytkowników są zaszyfrowane.
    e) Hasło do konta Administratora Danych Osobowych znane jest tylko administratorowi odpowiedzialnemu za dany system.
    f) Zastosowano metody kryptograficzne ochrony danych poprzez szyfrowanie dla danych osobowych przekazywanych drogą elektroniczną.
    g) Dane przekazywane są w obrębie bezpiecznych połączeń internetowych z wykorzystaniem protokołu SSL.
37. W zakresie zapewnienia integralności danych osobowych, administrator stosuje ponadto następujące środki techniczne i organizacyjne:
    a) pliki systemowe, a także relacyjna baza danych, poddawane są regularnym, zautomatyzowanym procedurom tworzenia kopii zapasowych.

§ 10

KONTROLA DOSTĘPU DO DANYCH

1. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych, a także do obsługi kartotek i dokumentów zawierających dane osobowe przetwarzanych w formie papierowej mogą zostać dopuszczone wyłącznie osoby posiadające upoważnienie administratora.
2. Dostęp do danych przyznaje się w oparciu o rolę jaką dana osoba pełni w związku z realizacją czynności wykonywanych w ramach zakresu obowiązków oraz poleceń administratora.
3. Dopuszcza się możliwość dostępu do danych przez podmioty zewnętrzne w przypadku zaistnienia okoliczności wynikających z obowiązujących przepisów prawa oraz zawartych umów lub upoważnień i nawiązanej współpracy przez Administratora. W odniesieniu do osób nie będących pracownikami, zasady ochrony i dostępu do danych są określone w odrębnych umowach lub uzgodnieniach, zaś nadzór nad przestrzeganiem wszelkich przepisów prawnych i uregulowań z zakresu ochrony danych spoczywa na właścicielu lub organie decyzyjnym podmiotu współpracującego.
4. Czas dostępu użytkownika do poszczególnych danych określony jest czasem wykonania zadania wynikającego z pełnionej roli.
5. Szczegółowy opis procesu zarządzania uprawnieniami do dostępu do danych osobowych i obsługi systemu informatycznego oraz nadawania, modyfikacji i anulowania uprawnień użytkowników realizowane są według zasad określonych w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych.
6. Osoby, które zostały upoważnione do przetwarzania danych osobowych obowiązane są do zachowania w tajemnicy tych danych oraz sposobów ich zabezpieczenia.
7. Przed uruchomieniem komputera na stanowisku pracy każdy użytkownik powinien dokonać przeglądu i sprawdzenia urządzeń komputerowych pod kątem ujawnienia okoliczności wskazujących na naruszenie dostępu do tych urządzeń lub danych zawartych na nich.
8. Praca w systemie informatycznym powinna być inicjowana właściwą dla danego systemu procedurą „login", która wymaga podania identyfikatora i hasła.
9. Jeśli istnieją możliwości techniczne, system informatyczny powinien wymuszać skończoną liczbę prób logowania, nie większą niż trzy.
10. Użytkownik opuszczając stanowisko pracy winien zwrócić szczególną uwagę na uniemożliwienie wykorzystywania systemu komputerowego przez osoby nieupoważnione, w szczególności na włączenie opcji wygaszacza ekranu po upływie ustalonego czasu nieaktywności użytkownika. Zaleca się ręczne blokowanie komputera przez użytkownika.
11. W przypadku zakończenia pracy, każdy użytkownik zobowiązany jest do:
    a. wykonania właściwej funkcji „logout",
    b. wyłączenia sprzętu komputerowego,
    c. zabezpieczenia stanowiska pracy, w szczególności dokumentacji i wymiennych nośników danych.

§ 11
ARCHIWIZACJA DANYCH OSOBOWYCH

1. Wszystkie bazy danych osobowych podlegają zabezpieczeniu i archiwizowaniu. Dane archiwizowane i przechowywane są przez czas wskazany dla poszczególnych kategorii danych osobowych.
2. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych baz danych oraz programów służących do przetwarzania danych.
3. Dostęp do kopii powinien być kontrolowany, przetwarzanie kopii archiwalnych powinno zapewniać ich poufność, integralność oraz dostępność.
4. Szczegółowe unormowania dotyczące tworzenia, przechowywania i usuwania kopii określa Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych.

§ 12
KONTROLA WEWNĘTRZNA I ZASADY POSTĘPOWANIA W PRZYPADKU NARUSZEŃ BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1. Do kontroli stanu ochrony danych osobowych uprawnieni są:
    a. Zarząd spółki WIK,
    b. Inspektora Ochrony Danych – w przypadku jego powołania,
    c. Administratora Systemów Informatycznych – w przypadku jego powołania,
    d. Pracownicy i inne podmioty upoważnione.

2. W przypadku przeprowadzenia kontroli przez użytkownika oraz stwierdzenia w czasie kontroli odstępstw od obowiązujących - na podstawie przepisów prawa i aktów prawnych wewnętrznych - zasad przetwarzania danych osobowych, użytkownik zobowiązany jest do poinformowania Zarządu spółki WIK i o wynikach kontroli i stwierdzonych faktach oraz uzgodnienia z nim dalszego toku postępowania.
3. Do zdarzeń zagrażających bezpieczeństwu danych osobowych należą:
    a) próby naruszenia ochrony danych:
        i. z zewnątrz – włamania do systemu, podsłuch, kradzież danych,
        ii. z wewnątrz – nieumyślna lub celowa modyfikacja danych, kradzież danych,
    b) programy destrukcyjne:
        i. wirusy,
        ii. konie trojańskie,
        iii. makra,
        iv. bomby logiczne,
    c) awarie sprzętu lub uszkodzenie oprogramowania,
    d) utrata zasilania powodująca przerwę w pracy systemów,
    e) zabór, utrata, uszkodzenie lub zniszczenie sprzętu lub nośników zawierających dane osobowe,
    f) inne skutkujące utratą danych osobowych, bądź wejściem w ich posiadanie osób nieuprawnionych (zjawiska fizyczne, takie jak powódź, pożar, huragan, działania silnych pół elektromagnetycznych, przechwycenie transmisji danych, odczyt danych z monitora komputera lub ekranu telefonu przez osoby nieuprawnione itp.).
4. W przypadku pozyskania informacji o fakcie nieprawnego przetwarzania, ujawnienia lub nienależytego zabezpieczenia przed osobami nieuprawnionymi danych osobowych, jak również stwierdzenia istnienia przesłanek wskazujących na prawdopodobieństwo naruszenia zasad ochrony danych osobowych, każdy użytkownik zobowiązany jest poinformować administratora, w celu umożliwienia przeprowadzenia lub koordynacji działań związanych z postępowaniem wyjaśniającym okoliczności danego zdarzenia. Na tyle, na ile jest to możliwe należy podjąć działania, które ograniczą rozmiar i dotkliwość naruszenia dla osób, których danych ono dotyczyło.
5. W ramach postępowania wyjaśniającego podejmowane są czynności mające na celu wyjaśnienie okoliczności danego zdarzenia, w szczególności:
    a) ustalenie czasu wystąpienia naruszenia, jego zakresu, przyczyn, skutków oraz wielkości szkód, które zaistniały,
    b) ustalenie osoby odpowiedzialnej za naruszenie,
    c) podjęcie działań w kierunku ograniczenia szkód oraz przeciwdziałania podobnym przypadkom w przyszłości,
    d) ocena naruszenia oraz podjęcie decyzji czy zachodzą obowiązkowe przesłanki do zgłoszenia wystąpienia naruszenia organowi nadzoru;
    e) wyciągnięcie konsekwencji w stosunku do osoby ponoszącej odpowiedzialność za zdarzenie, przy czym z tytułu przedmiotowych naruszeń możliwa jest m.in. odpowiedzialność:
        i. dyscyplinarna – na podstawie obowiązujących unormowań wewnętrznych,
        ii. cywilna – w oparciu o przepisy KC, w związku z wystąpieniem przez Administratora Danych Osobowych na drogę sądową,
        iii. karna,
    f) podjęcie decyzji czy zdarzenie spełnia przesłanki przestępstwa oraz czy ADO zobowiązany jest zgłosić sprawę do organów ścigania.
6. W trakcie prowadzenia postępowania wyjaśniającego osoba je prowadząca ma prawo do pełnej swobody działania, dostępu do dokumentów, wglądu do operacji wykonywanych w systemach informatycznych, pobierania wyjaśnień od pracowników i użytkowników oraz osób mogących mieć wpływ na wyniki postępowania oraz podejmowania wszelkich czynności mających na celu wyjaśnienie przyczyn, okoliczności i skutków zdarzenia oraz wskazania osób z nim powiązanych. Jeżeli przeprowadzającym postępowanie wyjaśniające nie jest zarząd spółki WIK, o wynikach postępowania należy go natychmiast poinformować.
7. Osoba prowadząca postępowanie wyjaśniające ma obowiązek jego przeprowadzenia i sporządzenia wyników, w czasie 48 godzin od powzięcia wiadomości o zdarzeniu.
8. Każde stwierdzone naruszenie musi zostać odnotowane w wewnętrznym rejestrze naruszeń, a te naruszenia, które zostały zaklasyfikowane jako charakteryzujące się większym niż niski stopniem powagi naruszenia, według przyjętych kryterium oceny, muszą zostać zgłoszone do Prezesa Urzędu Ochrony Danych Osobowych

niezwłocznie – nie później niż w ciągu 72 godzin od stwierdzenia naruszenia. Naruszenia, które zostały zaklasyfikowane jako charakteryzujące się wysokim lub bardzo wysokim stopniem powagi naruszenia, muszą zostać natychmiastowo zakomunikowane osobom, których danych one dotyczyły.

§ 13
POSTĘPOWANIE W PRZYPADKACH ZAGROŻEŃ I NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1. W przypadku nieprawidłowości w działaniu systemu, uszkodzenia lub podejrzenia o uszkodzenie sprzętu, oprogramowania, sieci telekomunikacyjnej lub danych należy bezzwłocznie powiadomić administratora.
2. W przypadku włamania lub podejrzenia o włamanie do systemu Administrator Systemu, do którego zostało skierowane zgłoszenie podejmuje działania w celu zabezpieczenia systemu i danych:
   a) zmienia hasła administracyjne,
   b) określa rodzaj i sposób włamania,
   c) podejmuje działania w celu uniemożliwienia ponownego włamania tego samego typu,
   d) szacuje straty,
   e) przywraca stan systemu sprzed włamania.
3. W przypadku uszkodzenia sprzętu lub programów z danymi, Administrator Systemu podejmuje działania w celu:
   a) określenia przyczyny uszkodzenia,
   b) oszacowania strat wynikających z ww. uszkodzenia,
   c) naprawy uszkodzeń, a w szczególności naprawy sprzętu, ponownego zainstalowania danego programu, odtworzenie jego pełnej konfiguracji oraz wczytania danych z ostatniej kopii zapasowej.
4. W przypadku uszkodzenia danych, Administrator Systemu podejmuje następujące działania:
   a) ustala przyczynę uszkodzenia danych,
   b) określa wielkość i jakość uszkodzonych danych,
   c) podejmuje działania w celu odtworzenia danych z ostatniej kopii zapasowej.
5. W przypadku zidentyfikowania osób odpowiedzialnych za wystąpienie któregoś ze zdarzeń zagrażających bezpieczeństwu danych, informacje o powyższym należy przekazać zarządowi spółki WIK.

Sporządzono w Rybniku, dnia 25 maja 2018 roku