POLITYKA BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH

w

Przedsiębiorstwie Inżynierii Sanitarnej „PIOTROWSKI” Spółka z ograniczoną odpowiedzialnością

Poznań, dnia 31 grudnia 2022 roku

§1

DEFINICJE POLITYKI BEZPIECZEŃSTWA

Ilekroć w dokumencie jest mowa o:

PIS lub **Podmiot** – należy przez to rozumieć **Przedsiębiorstwo Inżynierii Sanitarnej „PIOTROWSKI" Spółka z o.o. siedzibą w Poznaniu, ul. Starołęcka 31, 61-361 Poznań, KRS: 0000244356**.
Polityce bezpieczeństwa, dokumencie – należy przez to rozumieć politykę bezpieczeństwa w zakresie ochrony danych osobowych w PIS.
Ustawie – należy przez to rozumieć ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 z późn.zm.) lub późniejsze ustawy.
Rozporządzeniu – należy przez to rozumieć 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 późn. zm.).
Administratorze Danych - („AD") – należy przez to rozumieć Zarząd Przedsiębiorstwa Inżynierii Sanitarnej „PIOTROWSKI" Spółka z o.o.
Inspektor Ochrony Danych („IOD") – należy przez to rozumieć osobę wyznaczoną przez AD Przedsiębiorstwa Inżynierii Sanitarnej „PIOTROWSKI" Spółka z o.o. do nadzorowania i egzekwowania przestrzegania zasad ochrony danych osobowych.
Administratorze Systemu Informatycznego („ASI") – należy rozumieć przez to osobę odpowiedzialną za sprawne działanie systemu informatycznego, jego konserwację oraz wdrażanie niezbędnych zabezpieczeń gwarantujących bezpieczeństwo przetwarzanych danych osobowych.
Danych osobowych – należy przez to rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.
Zbiorze danych – należy przez to rozumieć każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

Przetwarzaniu danych – należy przez to rozumieć jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

Instrukcji Zarządzania Systemem Informatycznym – należy przez to rozumieć „Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w PIS.
Systemie informatycznym – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

Zabezpieczeniu danych w systemie informatycznym – należy przez to rozumieć wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

Usuwaniu danych – należy przez to rozumieć zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
Zgodzie osoby, której dane dotyczą – należy przez to rozumieć oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; zgoda może być odwołana w każdym czasie.
Odbiorcy danych - należy przez to rozumieć każdego, komu udostępnia się dane osobowe, z wyłączeniem:
a) osoby, której dane dotyczą,
b) osoby upoważnionej do przetwarzania danych,
c) przedstawiciela, o którym mowa w art. 31a,
d) podmiotu, o którym mowa w art. 31,
e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.
Osobie możliwej do zidentyfikowania – należy przez to rozumieć osobę, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.
Osobie upoważnionej – należy przez to rozumieć: pracownika, współpracownika, wolontariusza, praktykanta, stażystę w PIS posiadającego pisemne upoważnienie do przetwarzania danych osobowych nadane przez AD lub IOD w imieniu AD.
RODO oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) (Dz.Urz. UE L 119).
Podmiot przetwarzający oznacza organizację lub osobę, której Podmiot powierzył przetwarzanie danych osobowych (np. usługodawca IT, zewnętrzna księgowość).
RCPD lub Rejestr oznacza Rejestr Czynności Przetwarzania Danych Osobowych.

§2

ŹRÓDŁA POWSTANIA DOKUMENTU.

Niniejszy dokument zatytułowany „**Polityka bezpieczeństwa”** lub „**Polityka ochrony danych osobowych**” (dalej jako **Polityka**) ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych w **Przedsiębiorstwo Inżynierii Sanitarnej „PIOTROWSKI” Spółka z o.o.** (dalej jako PIS lub **Podmiot**).

Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO – rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) (Dz.Urz. UE L 119).

§3

CEL I ZAKRES STOSOWANIA POLITYKI BEZPIECZEŃSTWA.

Zadaniem niniejszego dokumentu jest ustanowienie i określenie zasad bezpieczeństwa dotyczących zbierania i przetwarzania danych osobowych w Podmiocie. Dokument ten

dotyczy wszystkich osób, które przetwarzają dane osobowe tj. zarówno pracowników, jak również współpracowników firmy tj. wszystkich osób, które przetwarzają dane osobowe w Podmiocie, bez względu na charakter tej współpracy.

Stosowanie zasad określonych w Polityce Bezpieczeństwa jest niezbędnym elementem ochrony danych osobowych przetwarzanych w Podmiocie i ma na celu zapewnienie prawidłową ochronę danych osobowych, poprzez uniemożliwienie jakiejkolwiek ingerencji osobom nieupoważnionym.

Polityka Bezpieczeństwa stosowana jest do następujących danych osobowych:

- dane przetwarzane w formie papierowej,

- dane przetwarzane na zewnętrznych nośnikach informacji,

- dane przetwarzane w systemie informatycznym.

Każda osoba, która w Podmiocie przetwarza dane osobowe, ma obowiązek zapoznania się z niniejszą Polityką Bezpieczeństwa, wraz z jej załącznikami i dokumentami powiązanymi.

§4

INTEGRALNE DOKUMENTY POWIĄZANE Z POLITYKĄ BEZPIECZEŃSTWA.

Integralnymi dokumentami powiązanymi z Polityką Bezpieczeństwa są wszystkie niezbędne wzory załączone do niniejszego dokumentu, jak również Polityka Prywatności i Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Podmiocie.

§5

BEZPIECZEŃSTWO PRZETWARZANIA DANYCH.

Bezpieczeństwo przetwarzania danych osobowych, w szczególności poprzez systemy informatyczne rozumuje się przez zapewnienie:

Poufności – zapewnieniu, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom,

Integralności – zapewnieniu, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

Rozliczalności – zapewnieniu, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,

Podczas przetwarzania danych osobowych w Podmiocie stosuje się wysoki poziom bezpieczeństwa, ponieważ urządzenia na których przetwarzane są dane osobowe połączone są z siecią publiczną.

Filary ochrony danych osobowych:

(1) **Legalność** – podmiot dba o ochronę prywatności i przetwarza dane zgodnie z prawem.

(2) **Bezpieczeństwo** – podmiot zapewnia odpowiedni poziom bezpieczeństwa danych podejmując stale działania w tym zakresie.

(3) **Prawa Jednostki** – podmiot umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.

(4) **Rozliczalność** – podmiot dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

Zasady ochrony danych

Podmiot przetwarza dane osobowe z poszanowaniem następujących zasad:

(1) w oparciu o podstawę prawną i zgodnie z prawem (legalizm);

(2) rzetelnie i uczciwie (rzetelność);

(3) w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);

(4) w konkretnych celach i nie „na zapas” (minimalizacja);

(5) nie więcej niż potrzeba (adekwatność);

(6) z dbałością o prawidłowość danych (prawidłowość);

(7) nie dłużej niż potrzeba (czasowość);

(8) zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

§6

OBOWIĄZKI ZWIĄZANE Z PRZETWARZANIEM DANYCH.

AD – zapewnia świadomość bezpieczeństwa przetwarzania danych osobowych w Podmiocie. Podejmuje odpowiednie działania zmierzające do prawidłowej ochrony danych osobowych. Wyznacza IOD i ASI. AD zobowiązany jest do wprowadzania procedur zapewniających prawidłowe przetwarzanie danych, jak również egzekwowanie rozwoju środków zapewniających prawidłowe przetwarzanie danych. Do AD należy również zapewnienie podstaw prawnych, jak również niezbędnych środków bezpieczeństwa przetwarzania danych osobowych od momentu ich zebrania do momentu ich usunięcia.

IOD – podlegając bezpośrednio pod AD, ma obowiązek nadzorować i egzekwować przestrzeganie zasad ochrony danych osobowych w systemach informatycznych, jak również w zbiorach prowadzonych w formie papierowej i elektronicznej. Jego zadaniem jest określenie wymogów bezpieczeństwa, nadzór nad wdrożeniem rozwiązań służących ochronie przetwarzania danych osobowych, prowadzenie dokumentacji polityki bezpieczeństwa, oraz wynikającej z niej procedur i instrukcji. IOD analizuje również przyczyny i okoliczności, naruszenia danych osobowych przygotowując dla AD zalecenia i rekomendacje dotyczące eliminacji ryzyka naruszenia bezpieczeństwa przetwarzania danych.

Osoby upoważnione do przetwarzania danych – do ich obowiązków należy zrozumienie, znajomość i stosowanie w jak największym, możliwym zakresie wszelkich środków związanych z ochroną danych osobowych, jak również uniemożliwienie dostępu do działań, osobom nieuprawnionym do przetwarzania danych osobowych. Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do tajemnicy danych osobowych, oraz informacji o sposobach ich zabezpieczenia. Do zadań osób przetwarzających dane osobowe należy również obowiązek informacyjny względem IOD, w momencie podejrzenia naruszenia, zauważenia naruszenia, lub wykrytych słabościach systemu przetwarzającego dane osobowe.

§7

OCHRONA DANYCH OSOBOWYCH – ZARZĄDZANIE.

Zasady ogólne związane z przetwarzaniem danych osobowych:

Każda osoba przetwarzająca dane osobowe w zakresie zgodnym z obowiązkami służbowymi jak również rolą sprawowaną w procesie przetwarzania danych odpowiada za bieżącą, operacyjną ochronę danych i przetwarzania ich w granicach jej upoważnienia.

Należy zapewnić poufność, integralność, rozliczalność w zakresie przetwarzania danych osobowych.

Każda osoba, która ma styczność z danymi osobowymi zobowiązana jest do ochrony danych osobowych.

Zgodnie ze zmieniającą się technologią – stosuje się adekwatny do tej technologii poziom bezpieczeństwa przetwarzania danych osobowych.

Upoważnienie do przetwarzania danych osobowych:

Przetwarzanie danych osobowych, może zostać udostępnione jedynie osobom, które posiadają upoważnienie od administratora danych, nadane na mocy obowiązujących przepisów prawa. Upoważnienie takie jest wydawane przez ADO – indywidualnie, przed rozpoczęciem przetwarzania danych osobowych.

W celu upoważnienia do przetwarzania danych osobowych, należy dostarczyć do ADO dokument – oświadczenie, którego wzór określa załącznik nr 1. niniejszej Polityki Bezpieczeństwa.

Na podstawie otrzymanego oświadczenia, IOD wydaje dokument upoważniający w sposób formalny do przetwarzania danych osobowych - upoważnienie do przetwarzania danych osobowych, którego wzór określa załącznik nr 2. niniejszego dokumentu.

W/w załączniki tj. załącznik nr 1. i załącznik nr 2. niniejszej Polityki Bezpieczeństwa przechowywane są w aktach osobowych pracowników i obowiązują do czasu ustania stosunku pracy, lub obowiązków związanych z przetwarzaniem danych osobowych.

Ewidencja osób upoważnionych:

Ewidencja osób upoważnionych do przetwarzania danych osobowych, jest na bieżąco aktualizowana przez IOD i zawiera (załącznik nr 3. Polityki Bezpieczeństwa):

- imię i nazwisko osoby upoważnionej do przetwarzania danych osobowych,

- stanowisko pracy osoby upoważnionej do przetwarzania danych osobowych,

- zakres upoważnienia do przetwarzania danych osobowych,

- datę nadania uprawnień do przetwarzania danych osobowych,

- datę zakończenia/odebrania uprawnień do przetwarzania danych osobowych,

- identyfikator, jeśli osoba upoważniona do przetwarzania danych osobowych jest zarejestrowana w systemie informatycznym, służącym do przetwarzania danych osobowych.

Bezpośredni przełożeni osób upoważnionych, zobowiązani są do natychmiastowego powiadomienia IOD, o cofnięciu, zakończeniu, odebraniu uprawnień do przetwarzania danych osobowych.

Wszystkie osoby przetwarzające dane osobowe zobowiązane są do zachowania tajemnicy dotyczącej przetwarzania danych osobowych, sposobów i form ich zabezpieczenia. Tajemnica ta obowiązuje w trakcie zatrudnienia jak również po ustaniu zatrudnienia.

Osoby, które zostały upoważnione do przetwarzania danych osobowych, zobowiązane są do zapoznania się z regulacjami wewnętrznymi dotyczącymi ochrony danych osobowych w podmiocie i podporządkowaniu się im. Dokumenty, które w szczególności opisują regulacje wewnętrzne to Polityka Bezpieczeństwa i Instrukcja Zarządzania Systemem Informatycznym.

Zgodność dokumentacji:

Niniejszy dokument musi być aktualizowany wraz ze zmieniającymi się przepisami prawa o ochronie danych osobowych, oraz wraz ze zmianami faktycznymi zachodzącymi w ramach podmiotu, które mogą skutkować nieaktualnymi lub nieadekwatnymi do stanu faktycznego zasadami ochrony danych osobowych zawartych w niniejszej dokumentacji. Okresowy przegląd Polityki Bezpieczeństwa, powinien mieć na celu stwierdzenie, czy niniejszy dokument spełnia wymogi aktualnej i planowej działalności podmiotu, oraz czy stan prawny na dzień dokonywania przeglądu jest aktualny. Zmiany w Polityce Bezpieczeństwa wymagają przeglądu wszystkich innych dokumentów związanych z ochroną danych osobowych w podmiocie.

§8

USŁUGI ZEWNĘTRZNE – ZARZĄDZANIE.

Bezpieczeństwo usług zewnętrznych związanych z przetwarzaniem danych osobowych.

Należy zapewnić, aby wszystkie usługi zewnętrzne były prowadzone zgodnie z wymaganiami bezpieczeństwa przetwarzania danych osobowych obowiązującymi w podmiocie wymaganiami umowy i wymaganiami prawa. Użytkownicy zewnętrzni, niebędący pracownikami podmiotu, powinni dostosować się do tych samych zasad bezpieczeństwa przetwarzania danych osobowych co użytkownicy będący pracownikami.

Wymagania bezpieczeństwa przetwarzania danych osobowych, zakres i poziom ich stosowania należy określić w umowie świadczenia usług.

Powierzenie przetwarzania danych osobowych.

Ewidencja powierzenia przetwarzania danych osobowych jest prowadzona w formie pisemnego wykazu udostępnień, zgodnie z załącznikiem nr 4 niniejszej Polityki Bezpieczeństwa.

Powierzenie przetwarzania danych osobowych musi zostać zawarte, wyłącznie w formie pisemnej. Forma ta powinna jednoznacznie określać zakres i cel przetwarzania danych, a także zakres odpowiedzialności z tytułu niewykonania umowy, lub nienależytego jej wykonania.

Powierzenie przetwarzania danych nie skutkuje zdjęciem odpowiedzialności z Podmiotu za zgodne przetwarzanie danych. W umowach, które stanowią podstawę powierzenia przetwarzania danych, albo eksploatacji systemu informatycznego, lub części infrastruktury systemu należy zamieścić zobowiązanie podmiotu zewnętrznego do przestrzegania niniejszego dokumentu, oraz zastosowania wszelkich niezbędnych środków technicznych i organizacyjnych, zapewniających odpowiedni poziom bezpieczeństwa przetwarzania danych.

Podmiot posiada zasady doboru i weryfikacji przetwarzających dane na jego rzecz opracowane w celu zapewnienia, aby przetwarzający dawali wystarczające gwarancje wdrożenia odpowiednich środków organizacyjnych i technicznych dla zapewnienia bezpieczeństwa, realizacji praw jednostki i innych obowiązków ochrony danych spoczywających na podmiocie.

Podmiot przyjął minimalne wymagania co do umowy powierzenia przetwarzania danych stosowane w ramach Polityki Bezpieczeństwa.

Podmiot rozlicza przetwarzających z wykorzystania podprzetwarzających, jak też z innych wymagań wynikających z Zasad powierzenia danych osobowych.

Udostępnienie danych osobowych.

Dane osobowe, mogą zostać udostępnione wyłącznie podmiotom, które są uprawnione do ich otrzymania na podstawie przepisów prawa, oraz osobom, których dotyczą. Udostępnienie danych osobowych może nastąpić wyłącznie za zgodą IOD lub ADO.

Informacje, które zawierają dane osobowe, powinny być przekazywane uprawnionym podmiotom lub osobom, za potwierdzeniem lub pokwitowaniem odbioru, ewentualnie innym bezpiecznym sposobem określonym wymogiem prawnym lub umową.

Udostępniając dane osobowe innym podmiotom należy każdorazowo odnotować w systemie informatycznym, z którego udostępniono dane lub w inny zatwierdzony sposób. Odnotować należy:

- Informacje o odbiorcy danych,

- zakresie udostępnionych danych,

- dacie udostępnienia danych.

Udostępniając dane osobowe należy pamiętać, aby poinformować odbiorcę że dane o których mowa, można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla podmiotu, dla którego zostały udostępnione.

Monitorowanie i przegląd usług.

Przegląd usług strony trzeciej powinien być udokumentowany i powinien zawierać informacje o poziomie wykonania usługi, incydentach bezpieczeństwa teleinformatycznego oraz ochrony danych osobowych, śladach audytowych, problemach operacyjnych, awariach, błędach i zakłóceniach.

§9

BEZPIECZEŃSTWO OBSZARÓW PRZETWARZANIA.

Obszar przetwarzania.

Dane osobowe mogą być przetwarzane tylko i wyłącznie, w miejscach gdzie Podmiot prowadzi działalność. Na pomieszczenia tej firmy składają się pomieszczenia biurowe lub części tych pomieszczeń, a w szczególności:

- pomieszczenia biurowe, w których zlokalizowane są archiwa, stacje robocze, lub serwery służące do przetwarzania danych osobowych,

- pomieszczenia w których przetrzymuje się dokumenty źródłowe, oraz wydruki z systemu informatycznego, które zawierają dane osobowe,

- pomieszczenia, w których przechowuje się sprawne i uszkodzone nośniki informacji, oraz kopie zapasowe zawierające dane osobowe.

Pomieszczenia biurowe, lub ich części w których przetwarzane są dane osobowe, powinny być zamykane na klucz w momencie nieobecności osób upoważnionych do przetwarzania danych osobowych, w sposób, który uniemożliwia dostęp osobom trzecim do tych danych. Osoby upoważnione zobowiązane są do zabezpieczenia pomieszczeń, ich części lub budynków w których przetwarzane są dane osobowe, na czas ich chwilowej nieobecności, jak również po zakończonej pracy. Klucze nie powinny być pozostawione w zamku drzwi, jak również nie można wynosić ich poza teren miejsca przeznaczonego do ich przechowywania.

Wydruki i nośniki elektroniczne, które zawierają dane osobowe, należy przechowywać w zamykanych szafach, które znajdują się w obszarach przetwarzania danych osobowych.

Niepotrzebne wydruki lub inne dokumenty związane z danymi osobowymi niszczone są za pomocą niszczarki.

Przebywanie w pomieszczeniach przetwarzania danych osobowych, osób postronnych jest możliwe tylko i wyłącznie w obecności osoby upoważnionej do przetwarzania tych danych.

Szczegółowy wykaz pomieszczeń i obszarów przetwarzania danych osobowych znajduje się w załączniku nr 5. niniejszego dokumentu.

Bezpieczeństwo środowiskowe.

Lokalizację i umiejscowienie danych osobowych dobiera się z uwzględnieniem wymaganych aspektów bezpieczeństwa dot. przetwarzania danych osobowych. W szczególności rozważa się aspekty dotyczące:

- zasilania energią energetyczną,

- klimatyzacji oraz wentylacji,

- wykrywania oraz ochrony przed pożarem i powodzią,

- fizycznej kontroli dostępu.

Pomieszczenia, w których przetwarza się dane osobowe wyposaża się w środki ochrony fizycznej i organizacyjnej chroniące przed nieautoryzowanym dostępem osób trzecich, uszkodzeniem danym, lub zakłóceniami w pracy. Kopie zapasowe zawierające dane osobowe, przetrzymywane są w innej fizycznej lokalizacji, w bezpiecznej odległości niż dane źródłowe.

Bezpieczeństwo urządzeń.

Urządzenia służące do przetwarzania danych osobowych, przechowywane są w miejscach nadzorowanych i bezpiecznych. Nie należy pozostawiać urządzeń mobilnych takich jak laptopy i smartfony, bez opieki jeżeli nie zastosowano w nich odpowiednich środków ochrony.

Fizyczna kontrola dostępu.

- Należy przestrzegać procedur eksploatacyjnych celem zabezpieczenia danych osobowych oraz dokumentacji systemu przed nieautoryzowanym i nieuprawnionym dostępem osób trzecich.

- Należy wdrożyć politykę czystego biurka i czystego ekranu celem redukcji ryzyka nieautoryzowanego i nieuprawnionego dostępu do danych osobowych.

- klucze dostępowe, hasła, karty etc. Służące do uzyskania dostępu do systemów informatycznych służących do przetwarzania danych osobowych należy zabezpieczyć, a sposób ich uzyskania należy szczegółowo zdefiniować w procedurach.

- dostęp do serwerowni i innych pomieszczeń, w których znajdują się systemy informatyczne służące do przetwarzania danych osobowych, lub zbiory nieinformatyczne należy rejestrować i celowo przeglądać, a przyznawanie dostępu do tych pomieszczeń gościom, należy wykonać wyłącznie w określonych celach, nadzorując cały ich pobyt w pomieszczeniach.

- Kończąc pracę, należy zabezpieczyć stanowisko pracy, chowając w zamykanych na klucz szafach, wszelkie nośniki informacji, dokumentację, wydruki etc.

- Monitory komputerów stacjonarnych, powinny zostać ustawione w taki sposób, aby uniemożliwiły podgląd wyświetlanych danych osobowych osobom nieuprawnionym.

- W przypadku korzystania z usług firm zewnętrznych w zakresie niszczenia dokumentów zawartej w formie papierowej jak i na nośnikach elektronicznych, należy wybrać firmę, cechującą się odpowiednimi zabezpieczeniami i doświadczeniem.

§10

OKRESOWE PRZEGLĄDY I OCENY RYZYKA.

Wszystkie systemy informatyczne i aplikacje powinny zostać poddane ocenie ryzyka pod kątem identyfikacji zagrożeń dla bezpieczeństwa przetwarzanych danych osobowych nie rzadziej niż raz na dwa lata. Ocena ryzyka powinna być również przeprowadzona, w momencie zmian procesów biznesowych systemów informatycznych i aplikacji.

Przeglądy bezpieczeństwa przetwarzania danych osobowych powinny być przeprowadzane okresowo nie rzadziej niż raz na dwa lata, w celu określenia wymaganego poziomu zabezpieczeń pozwalającego na ograniczenie ryzyka do poziomu akceptowalnego.

Przeglądy zgodności urządzeń informatycznych oraz sieci teleinformatycznych, z zasadami przetwarzania danych osobowych należy przeprowadzać nie rzadziej niż raz w roku.

Wszystkie narzędzia informatyczne służące do powyższych działań, powinny być chronione przed nieautoryzowanym dostępem, a ich użycie odpowiednio kontrolowane.

Analizy ryzyka i adekwatności środków bezpieczeństwa

Podmiot przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:

(1) Podmiot zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania – wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.

(2) Podmiot kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.

(3) Podmiot przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Podmiot analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych uwzględniając

charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

(4) Podmiot ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania, w tym Podmiot ustala przydatność i stosuje takie środki i podejście jak:

(i) pseudonimizacja,

(ii) szyfrowanie danych osobowych,

(iii) inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,

(iv) środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

Oceny skutków dla ochrony danych

Podmiot dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie.
Podmiot stosuje metodykę oceny skutków przyjętą przez siebie.

§11

ZARZĄDZANIE INCYDENTAMI.

Monitorowanie incydentów.

Wszystkie niezgodności związane z bezpieczeństwem przetwarzania danych osobowych, powinny być wykrywane, rejestrowane i monitorowane w celu ich usunięcia i zapobiegnięcia ponownemu wystąpieniu. Użytkownicy systemów w których przetwarza się dane osobowe powinni znać i przestrzegać zasady zgłaszania incydentów. Zgłaszane incydenty powinny być przechowywane jako materiał dowodowy.

Zgłaszanie incydentów.

Wszystkie zaistniałe zdarzenia związane z podejrzeniem naruszenia zasad bezpieczeństwa przetwarzania danych osobowych, lub naruszeniem zasad bezpieczeństwa przetwarzania danych osobowych takie jak np. utrata integralności, niedostępność, uszkodzenia, awarie, ostrzeżenia systemowe i alarmy bezpieczeństwa systemów informatycznych i urządzeń teleinformatycznych oraz danych, powinny niezwłocznie zostać zgłaszane do IOD

Podmiot stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych w terminie 72 godzin od ustalenia naruszenia.

§12

ZBIORY DANYCH OSOBOWYCH.

Wykaz zbiorów danych osobowych.

Dokumentacja związana ze zbiorami danych osobowych jest prowadzona w formie pisemnej przez IOD i stanowi załącznik nr 6. niniejszego dokumentu.

Wszystkie dane osobowe zebrane w zbiorach są przetwarzane w systemach informatycznych i w kartotekach informacyjnych. Zbiory te zlokalizowane są w pomieszczeniach lub ich częściach należących do obszaru przetwarzania danych osobowych.

Opis struktury zbiorów i sposób przepływu między poszczególnymi systemami.

Wskazane w załączniku nr 6. zakresy danych osobowych, które są przetwarzane w poszczególnych zbiorach danych osobowych, są ustalone w oparciu o strukturę zbiorów danych osobowych prowadzonych w systemach informatycznych, oraz powiązania pól informacyjnych utworzonych w tych systemach. Zawartość powyższych pól informacyjnych musi być zgodna z przepisami prawa, które uprawniają AD do przetwarzania danych.

Dokumentacja systemów informatycznych, w których przetwarzane są dane osobowe, powinna zawierać opis współpracy z innymi systemami informatycznymi, oraz powinna zawierać sposób przepływu danych pomiędzy poszczególnymi systemami, z którymi współpracuje. ASI zobowiązany jest do prowadzenia i uaktualniania dokumentacji opisującej sposób przepływu danych osobowych pomiędzy systemami.

Określenie zabezpieczeń technicznych i organizacyjnych.

Określenie zabezpieczeń niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych opisuje załącznik nr 7. niniejszej Polityki Bezpieczeństwa.

Rejestr Czynności Przetwarzania Danych

RCPD stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.

Podmiot prowadzi Rejestr Czynności Przetwarzania Danych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.

Rejestr jest jednym z podstawowych narzędzi umożliwiających Podmiotowi rozliczanie większości obowiązków ochrony danych.

W Rejestrze, dla każdej czynności przetwarzania danych, którą Podmiot uznał za odrębną dla potrzeb Rejestru, Podmiot odnotowuje co najmniej: (i) nazwę czynności, (ii) cel przetwarzania, (iii) opis kategorii osób, (iv) opis kategorii danych, (v) podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu Podmiotu, jeśli podstawą jest uzasadniony interes, (vi) sposób zbierania danych, (vii) opis kategorii

odbiorców danych (w tym przetwarzających), (viii) informację o przekazaniu poza EU/EOG; (ix) ogólny opis technicznych i organizacyjnych środków ochrony danych.

Wzór Rejestru stanowi **Załącznik nr ..... do Polityki – „Wzór Rejestru Czynności Przetwarzania Danych".**

Podmiot dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.

Wskazując ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel Podmiotu), dookreśla podstawę w czytelny sposób, gdy jest to potrzebne. Np. dla zgody wskazując na jej zakres, gdy podstawą jest prawo – wskazując na konkretny przepis i inne dokumenty, np. umowę, porozumienie administracyjne, żywotne interesy – wskazując na kategorie zdarzeń, w których się zmaterializują, uzasadniony cel – wskazując na konkretny cel, np. marketing własny, dochodzenie roszczeń.

Podmiot wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (email, telefon, sms, in.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).

§13

POSTANOWIENIA KOŃCOWE.

Niezależnie od odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego, naruszenie zasad niniejszej Polityki Bezpieczeństwa może być podstawą do rozwiązania stosunku pracy bez okresu wypowiedzenia z winy pracownika, który dopuścił się naruszenia przepisów.

W sprawach nieuregulowanych w niniejszej Polityce Bezpieczeństwa mają zastosowanie przepisy prawa powszechnie obowiązujące.

Wszyscy pracownicy Podmiotu przetwarzający dane osobowe, zobowiązani są do stosowania zasad bezpieczeństwa zawartych w niniejszym dokumencie. W przypadku przepisów wewnętrznych zawartych w innych procedurach, użytkownicy zobowiązani są do stosowania najwyższego poziomu ochrony danych osobowych.

Niniejszy dokument wchodzi w życie z dniem 25 maja 2018 roku

§14

Sposób obsługi praw jednostki i obowiązków informacyjnych

Podmiot dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.

Podmiot ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczenie na stronie internetowej Podmiotu informacji lub odwołań (linków) do informacji o prawach osób, sposobie skorzystania z nich, w tym wymaganiach dotyczących identyfikacji, metodach kontaktu z Podmiotem w tym celu, ewentualnym cenniku żądań „dodatkowych" itp.

Podmiot dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.

Podmiot wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.

W celu realizacji praw jednostki Podmiot zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Podmiot, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany,

Podmiot dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

§15

Obowiązki informacyjne

Podmiot określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.

Podmiot informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.

Podmiot informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.

Podmiot informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej.

Podmiot określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam gdzie to jest możliwe (np. tabliczka o objęciu obszaru monitoringiem wizyjnym).

Podmiot informuje osobę o planowanej zmianie celu przetwarzania danych.

Podmiot informuje osobę przed uchyleniem ograniczenia przetwarzania.

Podmiot informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).

Podmiot informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.

Podmiot bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

§16

Żądania osób

Prawa osób trzecich. Realizując prawa osób, których dane dotyczą, Podmiot wprowadza proceduralne gwarancje ochrony praw i wolności osób trzecich. W szczególności w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób (np. prawa związane z ochroną danych innych osób, prawa własności intelektualnej, tajemnicę handlową, dobra osobiste itp.), Podmiot może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.

Nieprzetwarzanie. Podmiot informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.

Odmowa. Podmiot informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.

Dostęp do danych. Na żądanie osoby dotyczące dostępu do jej danych, Podmiot informuje osobę, czy przetwarza jej dane oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych), a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych, z zastrzeżeniem, że kopii danych wydanej w wykonaniu prawa dostępu do danych Podmiot nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.

Kopie danych. Na żądanie Podmiot wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Podmiot wprowadza i utrzymuje cennik kopii danych, zgodnie z którym pobiera opłaty za kolejne kopie danych. Cena kopii danych skalkulowana jest w oparciu o oszacowany jednostkowy koszt obsługi żądania wydania kopii danych.

Sprostowanie danych. Podmiot dokonuje sprostowania nieprawidłowych danych na żądanie osoby. Podmiot ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Podmiot informuje osobę o odbiorcach danych, na żądanie tej osoby.

Uzupełnienie danych. Podmiot uzupełnia i aktualizuje dane na żądanie osoby. Ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. nie musi przetwarzać danych, które są mu zbędne). Podmiot może polegać na oświadczeniu osoby, co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Podmiot procedur (np. co do pozyskiwania takich danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

Usunięcie danych. Na żądanie osoby, Podmiot usuwa dane, gdy:

(1) dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,

(2) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,

(3) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,

(4) dane były przetwarzane niezgodnie z prawem,

(5) konieczność usunięcia wynika z obowiązku prawnego,

(6) żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku (np. profil dziecka na portalu społecznościowym, udział w konkursie na stronie internetowej).

Podmiot określa sposób obsługi prawa do usunięcia danych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w

tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art. 17. ust. 3 RODO.

Jeżeli dane podlegające usunięciu zostały upublicznione przez Podmiot, podejmuje on rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe, o potrzebie usunięcia danych i dostępu do nich.
W przypadku usunięcia danych Podmiot informuje osobę o odbiorcach danych, na żądanie tej osoby.

Ograniczenie przetwarzania. Podmiot dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:

a) osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,

b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,

c) Podmiot nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,

d) osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Podmiotu zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

W trakcie ograniczenia przetwarzania podmiot przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego.
Podmiot informuje osobę przed uchyleniem ograniczenia przetwarzania.

W przypadku ograniczenia przetwarzania danych Podmiot informuje osobę o odbiorcach danych, na żądanie tej osoby.

Przenoszenie danych. Na żądanie osoby Podmiot wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, **jeśli** jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona Podmiotowi, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych Podmiotu.

Sprzeciw w szczególnej sytuacji. Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Podmiot w oparciu o uzasadniony interes Podmiotu lub o powierzone mu zadanie w interesie publicznym, Podmiot **uwzględni** sprzeciw, o ile nie zachodzą po stronie Podmiotu ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

Sprzeciw przy badaniach naukowych, historycznych lub celach statystycznych. Jeżeli Podmiot prowadzi badania naukowe, historyczne lub przetwarza dane w celach statystycznych, osoba może **wnieść** umotywowany jej szczególną sytuacją sprzeciw względem takiego przetwarzania. Podmiot uwzględni taki sprzeciw, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

Sprzeciw względem marketingu bezpośredniego. Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Podmiot na potrzeby marketingu bezpośredniego (w tym **ewentualnie** profilowania), Podmiot uwzględni sprzeciw i zaprzestanie takiego przetwarzania.

Prawo do ludzkiej interwencji przy automatycznym przetwarzaniu. Jeżeli Podmiot przetwarza dane w sposób automatyczny, w tym w szczególności profiluje osoby, i w konsekwencji podejmuje względem osoby decyzje wywołujące skutki prawne lub inaczej istotnie wpływające na **osobę**, zapewnia możliwość odwołania się do interwencji i decyzji człowieka po stronie Podmiotu, chyba że taka automatyczna decyzja (i) jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą a Podmiotem; lub (ii) jest wprost dozwolona przepisami prawa; lub (iii) opiera się o wyraźną zgodę odwołującej osoby.

§17
PROJEKTOWANIE PRYWATNOŚCI

Podmiot zarządza zmianą mającą wpływ na prywatność w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz minimalizacji ich przetwarzania.
W tym celu zasady prowadzenia projektów i inwestycji przez Podmiot odwołują się do zasad bezpieczeństwa danych osobowych i minimalizacji, wymagając oceny wpływu na prywatność i ochronę danych, uwzględnienia i zaprojektowana bezpieczeństwa i minimalizacji przetwarzania danych od początku projektu lub inwestycji.

§18
DANE KONTAKTOWE

Kontakt z Administratorem jest możliwy poprzez adres e-mail iod@pis-piotrowski.pl lub adres korespondencyjny Przedsiębiorstwo Inżynierii Sanitarnej PIOTROWSKI Sp. z o.o.
ul. Starołęcka 31 | 61-361 Poznań.

Załącznik nr 1. Polityki Bezpieczeństwa – oświadczenie

....., dn. .....

OŚWIADCZENIE

Ja, niżej podpisana(y), oświadczam, że zapoznała(e)m się, rozumiem i będę przestrzegać obowiązków wynikających z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) (Dz.Urz. UE L 119) - RODO, ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.), aktów wykonawczych wydanych na jej podstawie, innych przepisów prawnych oraz dokumentów związanych z przetwarzaniem danych osobowych w **Przedsiębiorstwie Inżynierii Sanitarnej „PIOTROWSKI" Spółka z o.o.**, a w szczególności:

- Polityki Bezpieczeństwa,

- Instrukcji Zarządzania Systemem Informatycznym.

Zobowiązuje się do zapewnienia ochrony danym osobowym przetwarzanym zgodnie z ww. przepisami, a w szczególności zabezpieczę je przed dostępem osób nieupoważnionych, zabraniem, uszkodzeniem oraz nieuzasadnioną modyfikacją lub zniszczeniem

Zachowam w tajemnicy, także po ustaniu stosunku pracy lub kontraktu, wszelkie informacje dotyczące przetwarzania oraz sposobów zabezpieczenia danych osobowych w **Przedsiębiorstwie Inżynierii Sanitarnej „PIOTROWSKI" Spółka z o.o.**

Niezwłocznie zgłoszę przełożonemu lub Inspektorowi Ochrony Danych, jakąkolwiek próbę lub fakt naruszenia ochrony przetwarzanych danych osobowych.

Jednocześnie przyjmuje do wiadomości, że za niedopełnienie obowiązków wynikających z niniejszego oświadczenia, ponoszę odpowiedzialność na podstawie przepisów Regulaminu Pracy, Kodeksu Pracy, RODO oraz innych przepisów prawa powszechnie obowiązujących.

…… ……

(imię i nazwisko pracownika) (pracodawca)

Potwierdzam odbiór jednego egzemplarza oświadczenia.

……

(czytelny podpis pracownika)

Załącznik nr 2. Polityki Bezpieczeństwa – upoważnienie do przetwarzania danych osobowych.

....., dn. .....

UPOWAŻNIENIE

DO PRZETWARZANIA DANYCH OSOBOWYCH

Działając na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) (Dz.Urz. UE L 119)., nadaję
Pani/Panu*. . . . . zatrudnionej/zatrudnionemu*, na stanowisku . . . . . w **Przedsiębiorstwo Inżynierii Sanitarnej „PIOTROWSKI" Spółka z o.o.** upoważnienie do przetwarzania danych osobowych, wynikających z zakresu Pani/Pana* obowiązków służbowych oraz poleceń przełożonego.

Niniejsze upoważnienie wygasa z chwilą rozwiązania umowy o pracę lub z chwilą jego odwołania.

Jednocześnie zobowiązuję Panią/Pana* do zachowania w tajemnicy przetwarzanych danych osobowych oraz sposobu ich zabezpieczenia.

Upoważnienie obejmuje uprawnienie do przetwarzania danych osobowych zawartych w następujących zbiorach:

.....

.....

.....

Upoważnienie obejmuje uprawnienie do przetwarzania danych osobowych w następujących celach:

.....

.....

.....

....

(imię i nazwisko pracownika) (pracodawca)

Potwierdzam odbiór jednego egzemplarza upoważnienia.

.....

(czytelny podpis pracownika)

Załącznik nr 3. Polityki Bezpieczeństwa – ewidencja osób upoważnionych do przetwarzania danych osobowych.

L.p.	Imię i nazwisko	Stanowisko	Zakres przetwarzanych danych	Data nadania upoważnienia	Data końca upoważnienia	Identyfikator/Login w systemie informatycznym
1.						
2.						
3.						
4.						
5.						
6.						
7.						

POLITYKA BEZPIECZEŃSTWA
OCHRONY DANYCH OSOBOWYCH

Dokument stanowi przedmiot tajemnicy
Przedsiębiorstwa Inżynierii Sanitarnej
PIOTROWSKI Sp. z o.o.

Załącznik nr 4. Polityki Bezpieczeństwa – ewidencja powierzenia przetwarzania danych osobowych.

L.p.	Imię i Nazwisko	Data udostępnienia	Nazwa podmiotu, któremu udostępniono dane	Cel udostępnienia danych	Zakres udostępnionych danych	Rodzaj zbioru i lokalizacja zbioru
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						

POLITYKA BEZPIECZEŃSTWA
OCHRONY DANYCH OSOBOWYCH

Dokument stanowi przedmiot tajemnicy
Przedsiębiorstwa Inżynierii Sanitarnej
PIOTROWSKI Sp. z o.o.

Załącznik nr 5. Polityki Bezpieczeństwa - szczegółowy wykaz pomieszczeń i obszarów przetwarzania danych osobowych.

L.p.	Dokładna lokalizacja	Określenie pomieszczenia	Dział	Zabezpieczenia fizyczne pomieszczenia
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				

9.				

Załącznik nr 6. Polityki Bezpieczeństwa – ewidencja zbiorów danych osobowych.

L.p.	Nazwa zbioru	Cel przetwarzania zbioru	Nazwa systemu, ewidencji lub aplikacji, w której przetwarzane są dane osobowe	Opis struktury zbiorów danych	Sposób przepływu danych pomiędzy systemami
1.					
2.					

3.					

Załącznik nr 7. Polityki Bezpieczeństwa – określenie zabezpieczeń technicznych i organizacyjnych.

Dostęp do danych osobowych jest chroniony przy zastosowaniu następujących zabezpieczeń, niezbędnych dla zachowania poufności, integralności i rozliczalności przetwarzania danych osobowych.

1. **Ochrona pomieszczeń wykorzystywanych w celu przetwarzania danych osobowych – informacje dotyczące zastosowanych zabezpieczeń.**

a) Budynek i wszystkie pomieszczenia, w których przetwarzane są dane osobowe, zabezpieczony jest przed nieautoryzowanym dostępem osób nieuprawnionych.

b) Po zakończeniu pracy, dokumentacja w formie papierowej przechowywana jest w szufladach zamykanych na klucz.

c) Przebywanie w obszarach przetwarzania danych osobowych, osoby nieupoważnionej, możliwe jest tylko w obecności osoby upoważnionej do przetwarzania danych osobowych.

2. **Zabezpieczenie sprzętu komputerowego – informacje dotyczące zastosowanych zabezpieczeń.**

a) Dla zapewnienia ciągłości działania, stosowany jest sprzęt renomowanych firm.

b) Zbiory danych osobowych i programy służące do ich przetwarzania podlegają okresowym kopiom bezpieczeństwa.

c) Kopie bezpieczeństwa usuwane są niezwłocznie po ustaniu ich użyteczności.

3. **Ochrona transmisji danych – informacje dotyczące zastosowanych zabezpieczeń.**

a) W celu ochrony przetwarzania danych osobowych, przed zagrożeniami pochodzącymi z sieci publicznej stosuje się zabezpieczenia chroniące przed nieautoryzowanym dostępem.

b) Transmisja danych osobowych przez sieć publiczną jest zabezpieczona środkami ochrony kryptograficznej.

4. **Oprogramowanie systemów informatycznych – informacje dotyczące zastosowanych zabezpieczeń.**

a) W celu zapewnienia rozliczalności, każdy użytkownik systemu informatycznego posiada unikalny login/identyfikator i hasło użytkownika.

b) Hasło użytkownika składa się z minimum 8 znaków i zawiera małe i duże litery, cyfry lub znaki specjalne.

c) Hasła służące do uwierzytelniania w systemach informatycznych służących do przetwarzania danych osobowych zmienia się co najmniej raz na 30 dni. System informatyczny przypomina użytkownikowi o zmianie hasła.

5. **Narzędzia bazodanowe i inne narzędzia programowe – informacje dotyczące zastosowanych zabezpieczeń.**

a) Celem ochrony zbiorów danych osobowych prowadzonych w systemie informatycznym stosuje się mechanizmy kontroli dostępu.

b) System zapewnia informacje o użytkowniku i dacie pierwszego wprowadzenia , danych osobowych do systemu.

c) W momencie likwidacji nośników elektronicznych służących do przetwarzania danych osobowych stosuje się oprogramowanie przeznaczone do trwałego usunięcia danych, a dyski twarde niszczy się fizycznie.

6. **System użytkowany przez osobę uprawnioną do przetwarzania danych osobowych - informacje dotyczące zastosowanych zabezpieczeń.**

a) W celu zabezpieczenia przetwarzania danych osobowych, w celu krótkotrwałego opuszczenia stanowiska pracy, stosuje się blokadę ekranu zabezpieczonego hasłem.

b) Stosuje się mechanizmy kontroli dostępu zarówno do systemów jak i katalogów sieciowych.

c) Na stacjach roboczych użytkownicy nie posiadają uprawnień do nieautoryzowanego instalowania oprogramowania.

d) Stosuje się program antywirusowy z opcją automatycznego pobierania najnowszych definicji wirusów, jak i automatycznej aktualizacji.

e) Skanowaniu przez program antywirusy podlegają wszystkie nośniki magnetyczne i optyczne.

7. **Środki organizacyjne - informacje dotyczące zastosowanych zabezpieczeń.**

a) Prowadzona jest ewidencja osób, które przetwarzają dane osobowe.

b) Dostęp do danych osobowych możliwy jest po otrzymaniu formalnego upoważnienia do przetwarzania danych osobowych, wydane przez upoważnione osoby.

c) Wprowadzona zostaje Instrukcja Zarządzania Systemem Informatycznym.

d) Monitoruje się prace wdrożonych systemów zabezpieczeń systemów informatycznych.