POLITYKA OCHRONY DANYCH OSOBOWYCH

Podmiot: Pyrzyckie Przedsiębiorstwo Komunalne Sp. z o.o.

ADRES: Tadeusza Kościuszki 26, 74-200 Pyrzyce

SPIS TREŚCI

ROZDZIAŁ 1
Wstęp

§ 1

Celem Ogólnej Polityki Ochrony Danych Osobowych **zwanej dalej „Polityką”**, jest określenie zasad przetwarzania i zabezpieczania danych osobowych, aby uzyskać optymalny i zgodny z wymogami obowiązujących aktów prawnych sposób przetwarzania informacji zawierających dane osobowe.

§ 2

1. Polityka została opracowana w związku z wymogami zawartymi w art. 24 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

2. W razie zmiany obowiązujących przepisów prawa powodujących niezgodność niniejszego dokumentu z nimi, Polityka, oraz dokumenty z nią powiązane, zostaną dostosowane do obowiązujących przepisów.

§ 3

Ochrona danych osobowych realizowana jest poprzez zastosowanie zabezpieczeń fizycznych, opracowanie odpowiednich zasad przetwarzania danych, stosowanie oprogramowania systemowego i aplikacji oraz nadzór osób upoważnionych do przetwarzania danych.

§ 4

1. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w Pyrzyckim Przedsiębiorstwie Komunalnym Sp. z o.o. rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych.
2. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:
   1) poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
   2) integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   3) rozliczalność danych - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
   4) integralność systemu - rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;
   5) dostępność informacji - rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
   6) zarządzanie ryzykiem - rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

ROZDZIAŁ 2
Definicje

§ 4

Przez użyte w Polityce określenia należy rozumieć:

1) **Administrator** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;
2) **podmiot** – Pyrzyckie Przedsiębiorstwo Komunalne Sp. z o.o.;
3) **Inspektor ochrony danych (IOD)** – osoba wyznaczona przez Administratora, posiadająca kwalifikacje zawodowe, a w szczególności wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych osobowych oraz umiejętności wypełniania zadań wynikających z zapisów RODO;
4) **RODO** – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r w sprawie osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE;
5) **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
6) **zbiór danych osobowych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentalizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
7) **przetwarzanie danych** – operacja lub zestaw operacji wykonanych na danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie 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;
8) **upoważniony** – osoba będąca pracownikiem Administratora lub osoba wykonującą na rzecz Administratora usługi, która w związku z wykonywaniem czynności ma dostęp do danych osobowych, a do ich przetwarzania została pisemnie upoważniona przez Administratora;
9) **podmiot przetwarzający** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora, czyli działający na jego zlecenie;
10) **system informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
11) **system tradycyjny** – zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem danych osobowych zapisanych na papierze;
12) **zabezpieczenie danych w systemie informatycznym** – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
13) **administrator systemu informatycznego (ASI)** – osoba upoważniona przez Administratora do administrowania i zarządzania systemami informatycznymi;
14) **identyfikator użytkownika (login)** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

15) **hasło** – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

ROZDZIAŁ 3
Zakres i cel stosowania

§ 5

1. Administratorem jest: Pyrzyckie Przedsiębiorstwo Komunalne Sp. z o.o.
2. Osobą działającą w imieniu Administratora jest: Prezes Zarządu PPK Pyrzyce sp. z o. o.
3. Administrator odpowiedzialny jest za prawidłową organizację ochrony danych osobowych w podmiocie.
4. Administrator dokonał weryfikacji zasadności powołania IOD. Uwzględniając specyfikę i zakres przetwarzania danych osobowych w podmiocie został powołany **Inspektor ochrony danych**.

§ 6

1. W Pyrzyckim Przedsiębiorstwie Komunalnym Sp. z o. o. przetwarzane są przede wszystkim informacje związane z prowadzeniem PPK Pyrzyce (dane: klientów/kontrahentów, odbiorców usług, najemców lokali, pracowników PPK).
2. Informacje te są przetwarzane i składowane zarówno w postaci dokumentacji tradycyjnej jak i elektronicznej.
3. Polityka zawiera dokumenty dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

§ 7

Politykę stosuje się przede wszystkim do:

1. Danych osobowych przetwarzanych w systemie: ZSI Unisoft, R-2 Płatnik, Odpady, Abak Silver, Czynsze.
2. Wszystkich informacji dotyczących danych pracowników PPK Pyrzyce w tym danych osobowych pracowników i treści zawieranych umów o pracę.
3. Wszystkich danych kandydatów do pracy zbieranych na etapie rekrutacji.
4. Wszystkich danych stażystów.
5. Wszystkich danych członków Rady Nadzorczej.
6. Wszystkich danych klientów/kontrahentów, odbiorców usług, najemców lokali komunalnych.
7. Wszystkich danych osób skazanych – prace społecznie użyteczne.
8. Informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych.
9. Rejestru osób dopuszczonych do przetwarzania danych osobowych.
10. Innych dokumentów zawierających dane osobowe.

§ 8

1. Zakresy ochrony danych osobowych określone przez dokumenty Polityki mają zastosowanie do systemów informatycznych, w których są przetwarzane dane osobowe, a w szczególności do:
   1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie;
   2) wszystkich lokalizacji - budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie;
   3) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, osób fizycznych współpracujących na umowy zlecenie/o dzieło, stażystów i innych osób mających dostęp do informacji podlegających ochronie, w tym do członków zarządu.
2. Do stosowania zasad określonych przez dokumenty Polityki zobowiązani są wszyscy pracownicy w rozumieniu Kodeksu Pracy, stażyści oraz inne osoby mające dostęp do informacji podlegających ochronie, w tym członkowie zarządu.
3. Informacje niejawne nie są objęte zakresem niniejszej Polityki.

ROZDZIAŁ 4
Określenie miejsc i zbiorów

§ 9

1. Wykaz budynków i pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe zawiera **załącznik nr 1** do niniejszej Polityki.

§ 10

1. Administrator ma stały nadzór nad określanymi w **załączniku nr 2** do niniejszej Polityki zbiorami danych osobowych. Wykaz zbiorów danych zawiera informacje o:
   a) systemach informatycznych służących do przetwarzania poszczególnych zbiorów,
   b) podstawie prawnej przetwarzania danych (zasada legalności),
   c) terminie usuwania lub okresowych przeglądów danych pod kątem dalszej ich przydatności (zasada ograniczenia przechowywania).
2. Struktura zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych określona została w **załączniku nr 3** do niniejszej Polityki i podlega stałej weryfikacji pod kątem adekwatności gromadzonych danych w stosunku do celu przetwarzania (zasada minimalizacji)

ROZDZIAŁ 5
Obowiązek informacyjny

§ 11

1. W celu realizacji obowiązku informacyjnego Administrator, w przypadku pozyskiwania danych osobowych od osób fizycznych przedstawia klauzule informacyjne zawierające elementy takie jak:

- dane kontaktowe Administratora,
- cel przetwarzania danych,
- podstawa prawna przetwarzania (jeśli istnieje),
- okres przechowywania danych lub kryteria określenia tego okresu,
- informacje o prawach przyznanych przepisami prawa, np.: prawo do dostępu do swoich danych, prawo do sprostowania danych, prawo do odwołania zgody na przetwarzanie (jeśli zgoda jest podstawą do przetwarzania tych danych),
- informacje o prawie do wniesienia skargi do organu nadzorczego, gdy osoba, której dane dotyczą uzna, ze przetwarzanie jej danych odbywa się z naruszeniem przepisów ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.,
- informacje czy podanie danych jest warunkiem zawarcia umowy lub wymogiem ustawowym (jeśli dotyczy),
- informacje czy podanie danych jest obowiązkowe i jakie są ewentualne konsekwencje niepodania danych.

2. Klauzule informacyjne stosowane są w szczególności:
   - w procesie rekrutacji,
   - przy zatrudnianiu pracowników,
   - przy zawieraniu umów z osobami fizycznymi,
   - przy pozyskiwaniu danych poprzez formularze na stronach internetowych,
   - na wszelkich formularzach służących do pozyskiwania danych osobowych.
3. Administrator ma stały nadzór nad prawidłowym kształtem klauzul informacyjnych, dba o to, by były one czytelne, zrozumiałe i jasno przedstawiały informacje na temat procesu przetwarzania danych.

ROZDZIAŁ 6
Upoważnienia i ewidencja osób upoważnionych

§ 12

1. Do przetwarzania danych dopuszczone są wyłącznie osoby posiadające upoważnienie nadane przez Administratora. Wzór upoważnienia stanowi **załącznik nr 4** do niniejszej Polityki.
2. Administrator nadając uprawnienia pracownikom, którzy przetwarzają dane odbiera od pracownika oświadczenie o zachowaniu danych w poufności oraz o zapoznaniu się z przepisami i wewnętrznymi politykami określającymi zasady zabezpieczania i przetwarzania danych osobowych w podmiocie.
3. W celu nadzoru nad ważnością i zakresem upoważnień Administrator prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, która stanowi **załącznik nr 5** do niniejszej Polityki. Ewidencja zawiera informacje takie jak:
   a) imię i nazwisko upoważnionego,
   b) zakres upoważnienia,
   c) datę nadania upoważnienia,
   d) datę ustania upoważnienia (uzupełnianą w momencie odwołania upoważnienia – zakończenia stosunku pracy lub zmiany zakresu upoważnienia np. w przypadku zmiany stanowiska).

ROZDZIAŁ 7
Obowiązki osób upoważnionych i ich odpowiedzialność, ogólne zasady

§ 13

1. Pracownicy zobowiązani są przetwarzać dane zgodnie z prawem – wykorzystywać dane zgodnie z celem, dla którego zostały zebrane.
2. Należy zabezpieczać dane osobowe przed ich utratą, uszkodzeniem, zniszczeniem czy zmianą i nie udostępniać osobom nieupoważnionym.
3. Osoby upoważnione zobowiązuje się do stosowania określonych przez Administratora procedur i środków przetwarzania oraz zabezpieczania danych osobowych, a także do podporządkowania się poleceniom przełożonych w zakresie ochrony danych osobowych.
4. Zadaniem osoby upoważnionej jest dopilnowanie, by przebywanie osób nieupoważnionych w pomieszczeniach, w których przetwarzane są dane osobowe, miało miejsce wyłącznie w obecności osoby upoważnionej.
5. Dokumenty zawierające dane osobowe niezbędne do pracy w terenie należy przechowywać w warunkach gwarantujących ich należytą ochronę, tj. w teczkach uniemożliwiających odczytanie zawartości dokumentów.
6. Pozostawanie w pracy po godzinach pracy może mieć miejsce tylko w związku z pełnionymi obowiązkami i za zgodą Administratora lub osoby przez niego upoważnionej.
7. Po zakończeniu pracy:
   a) komputery wyłącza się, a komputery przenośne (w przypadku jego używania) zabezpiecza się w zamykanych szafkach,
   b) dokumenty zawierające dane osobowe zabezpiecza się poprzez zamknięcie w biurku/szafie, a klucze od biurek i szaf przechowuje się w uzgodnionym dla siebie miejscu,
   c) pomieszczenie zamyka się na klucz, zaraz po sprawdzeniu czy w pomieszczeniu nie pozostały niezabezpieczone dokumenty zawierające dane osobowe.
8. Pracownicy mają zachować szczególną ostrożność przy otwieraniu wiadomości mailowych zawierających załączniki, zwłaszcza w przypadku otrzymania wiadomości od nieznanego nadawcy.
9. W przypadku używania zewnętrznych nośników danych (pendrive, dyski zewnętrzne) na komputerach służbowych pracownik ponosi odpowiedzialność za skutki ich używania.
10. Pracownicy, których zakres obowiązków wymaga dokonywania czynności służbowych z dokumentacją zawierającą dane osobowe poza obszarem przetwarzania danych, a także czynności związanych z przesyłaniem i transportem korespondencji, są zobowiązani stosować środki zapewniające ochronę tych danych osobowych podczas ich transportu, przechowywania i użytkowania poza obszarem siedziby pracodawcy, a w szczególności zabezpieczyć te dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
11. W przypadku drukowania lub oczekiwania na wydrukowanie informacji zawierającej dane osobowe, upoważnionemu nie wolno odchodzić od drukarki, na której dokonywany jest wydruk, chyba, że w pomieszczeniu znajduje się inna upoważniona osoba lub drukarka znajduje się w zabezpieczonym miejscu chronionym przed dostępem osób nieupoważnionych.

12. Zabronione jest tworzenie dodatkowych kopii dokumentów zawierających dane osobowe, jeśli nie wymagają tego obowiązki służbowe.
13. Pracownicy w celu skutecznego usunięcia błędnie utworzonych lub niepotrzebnych już wydruków z danymi osobowymi mają obowiązek używać niszczarki do dokumentów. Obowiązkiem pracownika jest dopilnowanie, by przeznaczone do usunięcia dokumenty, zawierające dane osobowe niszczone były w stopniu uniemożliwiającym ich odczytanie.
14. W przypadku przejścia na inne stanowisko lub rozwiązania stosunku pracy, pracownik upoważniony do dostępu do danych osobowych zobowiązany jest rozliczyć się z dokumentów zawierających dane osobowe.
15. Zasady udzielania informacji przez telefon: Informacji telefonicznych nie udziela się, względnie udziela się po zidentyfikowaniu rozmówcy i stwierdzeniu jego upoważnienia do uzyskania danych:
    - ZOUKiEM, ZWiK, KSIĘGOWOŚĆ – identyfikacja klienta na podstawie imienia, nazwiska i numeru PESEL,
    - WINDYKACJA – identyfikacja klienta na podstawie imienia, nazwiska i numeru PESEL, ewentualnie numeru otrzymanego wezwania.
16. Zasady uzyskiwania i korzystania z numerów telefonów klientów indywidualnych. Podanie numeru telefonu przez klienta/kontrahenta jest dobrowolne. Numer telefonu może być pobrany w następujących sytuacjach:

    - w sytuacji zgłaszania telefonicznie awarii, numer telefonu będzie wykorzystywany tylko do kontaktu w sprawie awarii i po jej likwidacji, zostanie usunięty.
    - w sytuacji wykonywania przez PPK Pyrzyce jednorazowej usługi, numer telefonu będzie wykorzystywany tylko do kontaktu w sprawie usługi i jest usuwany po ostatecznym rozliczeniu usługi.
    - numer telefonu może być przekazany przez klienta w związku z zawieraniem i realizacją umów/zleceń (np. umowy na odbieranie nieczystości płynnych, odbierania nieczystości stałych, na dostawę wody i odprowadzanie ścieków, na wykonanie przyłączy wodociągowo-kanalizacyjnych, kwestii związanych z administrowaniem cmentarzami, np. przycinki gałęzi na cmentarzu, świadczenia usług pogrzebowych, kwestii związanych z zarządzaniem zasobami komunalnymi) w tym zapewnienia właściwej jakości świadczonych usług (np. usuwanie awarii). Podanie numeru i wyrażenie zgody na jego używanie jest dobrowolne i wymaga określenia celu dla jakiego zgoda została udzielona. Numer telefonu nie może być wykorzystywany dla celu innego niż na który udzielono zgody. Kopia podpisanej zgody na wykorzystanie numeru telefonu powinna być złożona u Inspektora Ochrony Danych Osobowych.
17. Ochrona wizerunku osób uczestniczących w konkursach/akcjach promocyjnych organizowanych przez PPK Pyrzyce.

    - regulamin konkursu/akcji promocyjnej winien zawierać w swojej treści klauzulę informacyjną dotyczącą ochrony danych osobowych.
    - w sytuacji wykonywania dokumentacji fotograficznej z wręczenia nagród z zamiarem publikacji zdjęć, konieczne jest pobranie od fotografowanych osób zgody na publikację wizerunku. Treść zgody opracowuje Inspektor Ochrony Danych Osobowych. Podpisane zgody należy złożyć u Inspektora ochrony Danych Osobowych.
18. Zabroniona jest publikacja wizerunku osób (pracowników, klientów, kontrahentów) bez uzyskania ich pisemnej zgody. Udzielenie zgody jest dobrowolne.

§ 14

1. Pracownicy, których zakres obowiązków wymaga dokonywania czynności służbowych z dokumentacją zawierającą dane osobowe poza obszarem przetwarzania danych, a także czynności związanych z przesyłaniem i transportem korespondencji ponoszą pełną odpowiedzialność za powierzony im sprzęt oraz dokumentację znajdującą się poza siedzibą Administratora.
2. Odpowiedzialność za bezpieczeństwo dokumentacji lub akt wynoszonych poza obszar przetwarzania danych ponosi pracownik, który te akta wynosi, z chwilą ich pobrania. Odpowiedzialność ta dotyczy również danych znajdujących się na nośnikach cyfrowych

ROZDZIAŁ 8
Szkolenia osób upoważnionych

§ 15

1. Każda osoba przed dopuszczeniem do pracy ze zbiorami danych osobowych w wersji papierowej lub mająca dostęp do systemu informatycznego służącego do przetwarzania danych osobowych zostaje poddana przeszkoleniu w zakresie ochrony danych osobowych.
2. Za zorganizowanie szkolenia odpowiada Inspektor Ochrony Danych.
3. Zakres szkolenia obejmuje zaznajomienie upoważnionego z przepisami z zakresu ochrony danych osobowych i wydanymi na ich podstawie wytycznymi oraz instrukcjami obowiązującymi u Administratora w zakresie zasad pracy z danymi osobowymi w zbiorach tradycyjnych i przetwarzanych za pomocą systemów informatycznych.
4. Szkolenia osób upoważnionych odbywają się cyklicznie, a powtarzane są zwłaszcza gdy:
   a) częste są uchybienia przy przetwarzaniu danych osobowych wynikające z zaniedbań pracowników,
   b) nastąpiła zmiana przepisów dotyczących przetwarzania i zabezpieczania danych osobowych.
5. Dokument zaświadczający odbycie szkolenia przechowywany jest w aktach osobowych pracownika.

ROZDZIAŁ 9
Udostępnienie i powierzanie danych osobowych

§ 16

1. W przypadku powierzenia przetwarzania danych osobowych Administrator korzysta wyłącznie z usług podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi prawa i chroniło prawa osób, których dane dotyczą.
2. Powierzenie przetwarzania danych może mieć miejsce na podstawie pisemnej umowy zawartej między Administratorem a podmiotem przetwarzającym, która określa w szczególności przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa

Administratora. Wzór umowy powierzenia danych stanowi **załącznik nr 6** do niniejszej Polityki.

3. W umowie powierzenia Administrator gwarantuje sobie prawo do osobistej lub zleconej (audyt zewnętrzny) kontroli wykonania przedmiotu umowy w siedzibie podmiotu przetwarzającego m. in. w zakresie odpowiedniego zabezpieczania danych oraz przestrzegania właściwych przepisów prawa.
4. Wykaz podmiotów, którym powierzono przetwarzanie danych stanowi **załącznik nr 7** do niniejszej Polityki.
5. Powierzenie przetwarzania danych uregulowane w Polityce nie ma zastosowania do przekazywania danych podmiotom upoważnionym do ich przetwarzania na mocy przepisów prawa, w tym w szczególności ZUS, Prokuraturze, Policji, Sądom, Komornikom, itd.

ROZDZIAŁ 10
Zasady zabezpieczenia danych osobowych

§ 17

1. Administrator jest odpowiedzialny za zastosowanie adekwatnych do istniejących zagrożeń zabezpieczeń. Zastosowane zabezpieczenia mają zminimalizować ryzyko wystąpienia niebezpiecznych zdarzeń – ograniczyć ryzyko zabrania danych przez osobę nieuprawnioną, uszkodzenia lub zniszczenia danych.
2. W podmiocie wprowadza się zabezpieczenia:
   a) organizacyjne – polegające na wprowadzeniu w placówce rozwiązań organizacyjnych zapewniających przejrzystość reguł zabezpieczających przetwarzane dane;
   b) techniczne – środki ochrony zawarte w oprogramowaniu, sprzęcie komputerowym i urządzeniach telekomunikacyjnych;
   c) fizyczne – zapewniające ochronę pomieszczeń i miejsc przechowywania danych osobowych, aby utrudnić ich naruszenie.
3. Wykaz wprowadzonych w podmiocie zabezpieczeń stanowi **załącznik nr 8** do niniejszej Polityki.

ROZDZIAŁ 11
Instrukcja postępowania w przypadku zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych

§ 18

1. Instrukcja definiuje katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Celem instrukcji jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.
2. Każdy pracownik Pyrzyckiego Przedsiębiorstwa Komunalnego Sp. z o.o. w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować Administratora.
3. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:

1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
2) niewłaściwe zabezpieczenie sprzętu, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
3) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników.

4. Do typowych incydentów bezpieczeństwa danych osobowych należą:
   1) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
   2) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/ zagubienie danych),
   3) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).
5. W przypadku stwierdzenia wystąpienia zagrożenia, Administrator prowadzi postępowanie wyjaśniające w toku, którego:
   1) ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki,
   2) inicjuje ewentualne działania dyscyplinarne,
   3) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości,
   4) dokumentuje prowadzone postępowania.
6. W przypadku stwierdzenia incydentu (naruszenia), Administrator prowadzi postępowanie wyjaśniające w toku, którego:
   1) ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały,
   2) zabezpiecza ewentualne dowody,
   3) ustala osoby odpowiedzialne za naruszenie,
   4) podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody),
   5) inicjuje działania dyscyplinarne,
   6) wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości,
   7) dokumentuje prowadzone postępowania.
7. Wzór raportu z postępowania stanowi **załącznik nr 9** do niniejszej Polityki.
8. W przypadku, gdy naruszenie bezpieczeństwa prowadzi do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych, które skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych Administrator ma obowiązek:
   1) zgłosić naruszenie do organu nadzorczego w trybie opisanym w art. 33 rozporządzenia (w ciągu 72 godzin od zdarzenia),
   2) zawiadomić osoby, które dane dotyczą, o naruszeniu ochrony danych osobowych w trybie opisanym w art. 34 rozporządzenia (bez zbędnej zwłoki, tak aby umożliwić tym osobom podjęcie niezbędnych działań zapobiegawczych).

§ 19

1. Każdy pracownik, który podejrzewa, iż mogło nastąpić naruszenie bezpieczeństwa ochrony danych osobowych lub podejrzewa próbę dokonania takiego naruszenia przez osoby nieupoważnione, jest zobowiązany do niezwłocznego poinformowania o powyższym

Inspektora Ochrony Danych, który prowadzi postępowanie kontrolne, pod kątem wyjaśnienia okoliczności ewentualnego naruszenia bezpieczeństwa danych osobowych.

2. Wobec osoby, która w przypadku stwierdzenia lub podejrzenia naruszenia bezpieczeństwa danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła osoby odpowiedzialnej za nadzorowanie naruszeń, lub nie stosuje się do obowiązków wynikających z wewnętrznych polityk można wszcząć postępowanie dyscyplinarne. Kara dyscyplinarna orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z przepisami oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

ROZDZIAŁ 12

§ 20

Realizacja praw określonych w art. 16-22 RODO

1. Osoba, której dane dotyczą, ma prawo żądania niezwłocznego sprostowania dotyczących jej danych osobowych. Wniosek o sprostowanie danych osobowych stanowi załącznik nr 11.
2. Osoba, której dane dotyczą ma prawo żądania niezwłocznego usunięcia dotyczących jej danych osobowych, w sytuacjach opisanych w art. 17 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE. Wniosek o usuniecie danych osobowych stanowi załącznik nr 12.
3. Osoba, której dane dotyczą ma prawo żądania ograniczenia przetwarzania danych osobowych w przypadkach opisanych w art. 18 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE. Wniosek o ograniczenie przetwarzania danych osobowych stanowi załącznik nr 13.
4. Osoba, której dane dotyczą ma prawo do przeniesienia danych zgodnie z art. 20 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie osób fizycznych w związku z przetwarzaniem danych osobowych i w

sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE. Wniosek o przeniesienie danych osobowych stanowi załącznik nr 14.

5. Formularze dostępne są w działach ZOUKiEM, ZWiK, ZZK oraz u Inspektora Ochrony Danych Osobowych.
6. W sytuacji otrzymania wniosku jest on przekazywany do biura prawnego w celu wystawienia opinii, odnośnie zasadności wniosku oraz przygotowywana jest odpowiedź. Odpowiedź przekazywana jest drogą listowną.

ROZDZIAŁ 13

§ 21

Postanowienia końcowe

1. W sprawach nieuregulowanych w wewnętrznych politykach Administratora mają zastosowanie przepisy prawa z zakresu ochrony danych osobowych.
2. Administrator dokonuje systematycznej analizy wdrożonych dokumentów z zakresu ochrony danych osobowych w celu oceny ich aktualności i ewentualnej ich aktualizacji. Analiza taka dokonywana jest nie rzadziej niż raz w roku.
3. Wszyscy pracownicy upoważnieni do przetwarzania danych osobowych zobowiązani są do zapoznania się z niniejszą Polityką oraz do stosowania reguł w niej zawartych.
4. Wykaz osób zapoznanych z wewnętrznymi zasadami ochrony danych osobowych stanowi **zał. nr 10** do niniejszej Polityki.
5. Integralną część niniejszej Polityki stanowią załączniki:

Zał. nr 1 – Wykaz budynków i pomieszczeń
Zał. nr 2 – Wykaz zbiorów danych
Zał. nr 3 – Opis struktury zbiorów danych
Zał. nr 4 – Wzór upoważnienia do przetwarzania danych
Zał. nr 5 – Ewidencja osób upoważnionych
Zał. nr 6 – Wzór umowy powierzenia danych
Zał. nr 7 – Wykaz podmiotów, którym powierzono przetwarzanie danych
Zał. nr 8 – Wykaz wprowadzonych zabezpieczeń
Zał. nr 9 – Wzór raportu z naruszenia bezpieczeństwa danych osobowych
Zał. nr 10 – Wykaz osób zapoznanych z zapisami wewnętrznych polityk
Zał. nr 11 – Wniosek o sprostowanie danych osobowych
Zał. nr 12 – Wniosek o usuniecie danych
Zał. nr 13 – Wniosek o ograniczenie przetwarzania danych

§ 22

Niniejszy dokument wchodzi w życie z dniem 30.07.2019

Podpis:

……
Administrator

załącznik nr 1

Wykaz budynków i pomieszczeń

Dane osobowe przetwarzane są w budynku mieszczącym się przy ul. Kościuszki 26 w Pyrzycach

Parter

Lp.	Nr pokoju	Dział użytkujący pomieszczenie	Rodzaj zabezpieczenia fizycznego
1.		Prezes Zarządu	Drzwi zamykane na klucz, szafki zamykane na klucz.
2.	Pok. 1	Księgowość	Metalowe drzwi zamykane na klucz.
3.	Pok. 2	Zastępca Głównego Księgowego St. Inspektor ds. płac i rozliczeń	Drzwi zamykane na klucz, szafki zamykane na klucz.
4.		Kasjer	Drzwi zamykane na klucz, kraty w oknach, szafa pancerna.
5.	Pok. 3	Inspektor d.s. finansowo księgowych	Drzwi zamykane na klucz, szafki zamykane na klucz.
6.		Centrala telefoniczna	Drzwi zamykane na klucz, szafki zamykane na klucz, UPS.
7.		Archiwum	Drzwi zamykane na klucz, siatka zabezpieczająca w oknach.
8.	Pok. 6	Kierownik działu d.s. pracowniczych i administracji Starszy inspektor d.s. BHP	Drzwi zamykane na klucz, szafki zamykane na klucz, szafa pancerna.
9.	Pok. 7	Zakład wodociągów i kanalizacji Kierownik działu	Drzwi zamykane na klucz, szafki zamykane na klucz.
10.	Pok. 8	Zakład wodociągów i kanalizacji	Drzwi zamykane na klucz, szafki zamykane na klucz.
11.	Pok. 9	Zakład Wodociągów i Kanalizacji - inkasenci	Drzwi zamykane na klucz, szafki zamykane na klucz
12.	Pok. 10,11	Zarządzanie zasobami komunalnymi	Drzwi zamykane na klucz, szafki zamykane na klucz.
13.	Pok. 12	Inspektor d.s. Administracji i windykacji	

			Drzwi zamykane na klucz, szafki zamykane na klucz.
14.	**Pok. 13**	**Główny specjalista ds. ochrony środowiska**	**Drzwi zamykane na klucz, szafki zamykane na klucz.**
15.	**Pok. 14**	**Inspektor d.s. administracyjnych i zaopatrzenia**	**Drzwi zamykane na klucz, szafki zamykane na klucz.**
16.	**Pok. 17**	**Sekretariat**	**Drzwi zamykane na klucz, szafki zamykane na klucz,**
		Główny specjalista ds. zamówień publicznych. Inspektor ds. ochrony danych osobowych	**Drzwi zamykane na klucz, szafki zamykane na klucz, szafa metalowa zamykana na klucz.**
17.	**Pok. 18**	**Kierownik ZOUKiEM**	**Drzwi zamykane na klucz, szafki zamykane na klucz.**
18.	**Pok.19**	**Zarząd obsługi urządzeń komunalnych i estetyki miast**	**Drzwi zamykane na klucz, szafki zamykane na klucz.**
19.		**Magazyn**	**Kraty w oknach szafki zamykane na klucz, drzwi zamykane na klucz.**

Dane osobowe przetwarzane są w budynku mieszczącym się przy ul. Stargardzkiej w Pyrzycach (oczyszczalnia ścieków)

Lp.	Nr pokoju	Dział użytkujący pomieszczenie	Rodzaj zabezpieczenia fizycznego
1.	**Pokój kierownika**	**Z-ca kierownika ds. oczyszczalni ścieków. Technolog-laborant**	**Drzwi zamykane na klucz, szafki zamykane na klucz.**
2.	**Dyspozytornia**	**Z-ca kierownika ds. oczyszczalni ścieków. Technolog-laborant. Maszynista oczyszczalni ścieków.**	**Drzwi zamykane na klucz.**

załącznik nr 2

Wykaz zbiorów danych osobowych

Lp.	Nazwa zbioru danych	Przetwarzanie danych w systemie		Podstawa legalnego przetwarzania	Termin usuwania danych ze zbioru lub okresowego przeglądu przydatności danych
		tradycyjnym (zaznaczyć „X”)	informatycznym (wskazać nazwę)		
1.	Dane pracownicze	X	MS OFFICE	**TECZKI OSOBOWE** - Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2018 r., poz. 108 t.j.) - w szczeg. art. 22 z ind. 1 w związku z art. 94 pkt 9a i 9b	50 lat [art. 51u ust. 1 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2018 r., poz. 217 t.j.)]
			ZSI UNISOFT	**PŁACE** - Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2018 r. poz. 108 t.j.) Dział III - Wynagrodzenia; ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz.U. z 2017 r., poz. 1778 t.j.) - art. 1, 6 oraz 6a;	50 lat [art. 125a ust. 4 ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz.U.z 2017 r., poz.1383)]
			ZUS PŁATNIK	**ZGŁOSZENIA DO ZUS** - Ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz.U. z 2017 r., poz. 1778 t.j.) - art. 1, 6 oraz 6a"	50 lat [art. 125a ust. 4 ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz.U.z 2017 r., poz.1383)]
2.	Kandydaci do pracy (CV)	X	Office, program pocztowy	Kodeks pracy (art. 22 par.1)/ zgoda osoby, której dane dotyczą	Po zakończeniu procesu rekrutacji

3.	Stażyści	X		Na podstawie umów z Powiatowym Urzędem Pracy (programy aktywizacji osób bez pracy w powiecie pyrzyckim) Dane wykorzystywane tylko w celach realizacji umowy	Zgodnie z umowa zawartą z Powiatowym Urzędem Pracy. Zazwyczaj 10 lat.
4.	Dane członków Rady Nadzorczej	X	ZUS PŁATNIK, ZSI UNISOFT	**ZGŁOSZENIA DO ZUS** - Ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz.U. z 2017 r., poz. 1778 t.j.) - art. 1, 6 oraz 6a"	50 lat [art. 125a ust. 4 ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz.U.z 2017 r., poz.1383)]
5.	Umowy	X	ZSI UNISOFT,	Osoba, której dane dotyczą jest stroną umowy	5 lat od zakończenia umowy
6.	Faktury	X	ZSI Unisoft, Abak Silver	Przepisy podatkowe	6 lat
7.	Przetargi	X		Ustawa z dnia 29 stycznia 2004 r. Prawo zamówień publicznych Dz.U. 2017 poz. 1579. Rozporządzenie Ministra Rozwoju z dnia 26.VII.2016 w sprawie rodzaju dokumentów jakich może żądać zamawiający od wykonawców w postępowaniu o udzielenie zamówienia publicznego.	4 lata od zakończenia postępowania o zamówieniu publicznym.
8.	Prace osób skazanych	X		Rozporządzenie Ministra Sprawiedliwości w sprawie podmiotów, w których jest wykonywana kara ograniczenia wolności	Po odbyciu kary orzeczenia sądowe (skierowanie do odbycia kary) są odsyłane do Sądu.

				oraz praca społecznie użyteczna. Dz.U. 2018.98.634 z dnia 07.06.2010.	
9.	Dłużnicy - Windykacje	X	ZSI Unisoft	Art. 115 par. 12, art. 190a, art. 191 ustawy z 6 czerwca 1997 r. – Kodeks karny (Dz.U. z 1997 r. nr 88, poz. 553 z późn. zm.).	
10.	Składnica Akt	X		Ustawy z dnia 14 lipca 1983 roku o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2018 r., poz. 217)	
11.	ZFŚS	X		Ustawa z dnia 4 marca 1994 r. o zakładowym funduszu świadczeń socjalnych.	
12.	Dziennik Korespondencji (Registratura)	X	ZSI Unisoft	Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz. U. Nr 14, poz. 67 z 2011 r.)	
13.	Monitoring		CCTV	Zgoda osoby której dane dotyczą	
14.	Najemcy lokali	X	Czynsze	Osoba której dane dotyczą jest stroną umowy	
15.	Klienci/kontrahenci	X	ZSI Unisoft	Osoba której dane dotyczą jest stroną umowy	

16.	Odbiorcy usług	X	ZSI Unisoft	Osoba której dane dotyczą jest stroną umowy	
17.	Przyłącza sieci/awarie	X	ZSI Unisoft	Osoba której dane dotyczą jest stroną umowy	

załącznik nr 3

Opis struktury zbiorów danych

Lp.	Nazwa zbioru danych	Struktura zbioru
1.	Dane pracownicze	Imiona, Nazwisko, Nazwisko rodowe, Data urodzenia, Miejsce urodzenia, Imię ojca, Imię matki, PESEL, NIP, Właściwy oddział NFZ, Numer telefonu, Adres e-mail, Adres zameldowania (ulica, miejscowość, kod pocztowy, gmina), Adres zamieszkania (ulica, miejscowość, kod pocztowy, gmina), Adres do korespondencji (ulica, miejscowość, kod pocztowy, gmina), Stan cywilny, Zawód, Wykształcenie, Dane właściwego urzędu skarbowego, Informacja o stawkach podatkowych (standardowych, indywidualnych, opodatkowaniu wspólnie z małżonkiem), Dane dotyczące dokumentu tożsamości (rodzaj, seria i numer, data wydania, data ważności), Obywatelstwo, Numer rachunku bankowego, Oświadczenia i dane związane z obowiązkowym ubezpieczeniem społecznym. Oświadczenia i dane związane z dobrowolnym ubezpieczeniem społecznym, Dane dotyczące badań lekarskich wykonanych przez pracownika, Dane dotyczące odbytych przez pracownika szkoleń BHP
2.	Kandydaci do pracy (CV)	Imię, nazwisko, miejsce zamieszkania, nr. telefonu, adres e-mail, data urodzenia, wykształcenie, przebieg zatrudnienia
3.	Stażyści	Imię, nazwisko, miejsce zamieszkania, data urodzenia, wykształcenie, PESEL
4.	Dane członków Rady Nadzorczej	Imię, nazwisko, miejsce zamieszkania, data urodzenia, PESEL, nr telefonu
5.	Umowy	Osoba fizyczna: Imię, nazwisko, adres, nr dowodu, PESEL, nr telefonu Osoba fizyczna prowadząca działalność: Nazwa, imię, nazwisko, adres, NIP, nr telefonu
6.	Faktury	Osoba fizyczna: Imię, nazwisko, adres, PESEL Osoba fizyczna prowadząca działalność: Nazwa, imię, nazwisko, adres, NIP

7.	Przetargi	Imię, nazwisko, wykształcenie, uprawnienia zawodowe
8.	Prace osób skazanych	Imię, nazwisko, adres zamieszkania, data urodzenia
9.	Dłużnicy - Windykacje	Imię nazwisko, adres zamieszkania, numer i seria dowodu osobistego, PESEL, nr telefonu
10.	Składnica Akt	Dane ze wszystkich zbiorów.
11.	ZFŚS	Imię nazwisko , wysokość dochodu
12.	Dziennik Korespondencji (registratura)	Imię, nazwisko, Adres
13.	Monitoring	Wizerunek Osoby Fizycznej
14.	Najemcy lokali	Imię, nazwisko, adres, nr telefonu, nr i seria dowodu osobistego, PESEL, nr telefonu
19.	Klienci/kontrahenci	Imię, nazwisko, adres, PESEL, nr telefonu
20.	Odbiorcy usług	Imię, nazwisko, adres, PESEL, nr telefonu
21.	Przyłącza sieci/awarie	Imię, nazwisko, adres, PESEL, nr telefonu

załącznik nr 4

Wzór upoważnienia do przetwarzania danych osobowych nr ……

Administrator: **Pyrzyckie Przedsiębiorstwo Komunalne Sp. z .o.o.**

dnia …… nadaje upoważnienie

dla: ……..……..

stanowisko służbowe: ……

Upoważniony otrzymuje dostęp do zasobów danych osobowych w celu ich przetwarzania zgodnie z poleceniem wynikającym z zakresu obowiązków służbowych:

LP.	ZBIÓR DANYCH	DOSTĘP (X – tak)	ZAKRES: **wg** – wgląd, **wp** – wprowadzanie, **e** – edycja, **k** – kopiowanie, **u** – usuwanie, **ud** – udostępnianie
1.	Dane pracownicze		
2.	Kandydaci do pracy (CV)		
3.	Stażyści		
4.	Dane członków Rady Nadzorczej		
5.	Umowy		
6.	Faktury		
7.	Przetargi		
8.	Prace osób skazanych		
9.	Dłużnicy -Windykacje		
10.	Składnica Akt		
11.	ZFŚS		
12.	Dziennik Korespondencji (registratura)		
13.	Monitoring		
14.	Najemcy lokali		
15.	Klienci/kontrahenci		

16.	Odbiorcy usług		
17.	Przyłącza sieci/awarie		

Upoważnienie nadaje się do ustania stosunku pracy. Wszelakie poprzednie upoważnienia do przetwarzania danych osobowych z dniem wprowadzenia niniejszego wygasają. Jednocześnie bieżące upoważnienie zostaje zawieszone w przypadku nieobecności / urlopu przekraczającego 30 dni kalendarzowych. Po upływie w/w okresu nieobecności / urlopu upoważniony(a) wykonując obowiązki wynikające z upoważnienia otrzymuje ponowne upoważnienie niniejszym dokumentem.

OŚWIADCZENIE UPOWAŻNIONEGO

Ja niżej podpisany/a, oświadczam, że zostałem/am zaznajomiony/a z przepisami dotyczącymi ochrony danych osobowych i z wprowadzonymi zasadami ochrony danych osobowych zapisanymi w wewnętrznych politykach oraz zobowiązuję się do ich przestrzegania.

Jednocześnie oświadczam, że:

1. Zobowiązuję się do zachowanie w tajemnicy danych osobowych, do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań służbowych i obowiązków pracowniczych, zarówno w trakcie wiążącego mnie stosunku pracy, jak i po ustaniu zatrudnienia.
2. Zapewnię ochronę danym przetwarzanym, a w szczególności zabezpieczę je przed dostępem osób nieupoważnionych, zabraniem, uszkodzeniem oraz nieuzasadnioną modyfikacją lub zniszczeniem.
3. Natychmiast zgłoszę stwierdzenie próby lub faktu naruszenia zasad ochrony danych osobowych lub bezpieczeństwa systemy informatycznego, w którym przetwarzane są dane osobowe.
4. Przyjmuję do wiążącej wiadomości, iż postępowanie rażąco sprzeczne z wyżej wskazanymi obowiązkami i przepisami prawa, może być uznane za ciężkie naruszenie obowiązków pracowniczych.

Podpisy:

…… ……..

Administrator Osoba upoważniona

załącznik nr 5

Ewidencja osób upoważnionych do przetwarzania danych osobowych

Lp.	Imię i nazwisko	Zakres upoważnienia	Data nadania	Data ustania

załącznik nr 6

Wzór umowy powierzenia przetwarzania danych

zwana dalej „Umową”,

zawarta w …….., dnia ..... r.

pomiędzy:

……..

Reprezentowana przez: …….

zwanym dalej „Administratorem”

a

……..,

zwanym dalej „Podmiotem przetwarzającym”,

zwanymi łącznie „Stronami”.

Mając na uwadze, iż Strony łączy Umowa z dnia ....., przedmiotem której jest ……. zwana dalej „Umową główną”, w trakcie wykonywania której przetwarzane są dane osobowe, Strony zgodnie postanowiły, co następuje:

§ 1

Przedmiot Umowy

1. Strony postanawiają, że w celu spełnienia obowiązków wynikających z art. 28 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. zwanego dalej „Rozporządzeniem”, Administrator powierza Podmiotowi przetwarzającemu dane osobowe w celu realizacji Umowy głównej.
2. Zakres przetwarzania obejmuje ……... *(np. wgląd, edycję, udostępnianie, archiwizację)* danych osobowych w zbiorach Administratora: …….. *(np. Dane pracownicze)*
3. Przetwarzane dane dotyczą …….. *(pracowników, klientów itp.)*
4. Przetwarzane dane obejmują: …… *(imię, nazwisko, adres, PESEL, wizerunek itp.)*

§ 2

Obowiązki i prawa Administratora

1. Administrator powierzone Podmiotowi przetwarzającemu do przetwarzania dane osobowe gromadzi zgodnie z obowiązującymi przepisami prawa oraz jest uprawniony do powierzenia przetwarzania danych osobowych.
2. Administrator zobowiązany jest do przekazywania danych zachowując zasady bezpieczeństwa w celu zachowania poufności i integralności powierzanych danych.

3. Administrator zezwala / nie zezwala na korzystanie przez Podmiot przetwarzający z usług innego podmiotu przetwarzającego.
4. Administrator ma możliwość wyrażenia sprzeciwu wobec dodania lub zastąpienia innych podmiotów przetwarzających.
5. Administrator ma prawo samodzielnie lub za pomocą upoważnionych przez siebie audytorów przeprowadzić audyty lub inspekcje, których celem jest weryfikacja realizacji obowiązków wynikających z zapisów Rozporządzenia.

§ 3

Obowiązki Podmiotu przetwarzającego

1. Podmiot przetwarzający przy przetwarzaniu powierzonych danych osobowych zobowiązany jest stosować przepisy Rozporządzenia, w tym:
   a) stosować środki techniczne i organizacyjne zapewniające bezpieczeństwo powierzanym danym, w stopniu adekwatnym do ryzyka występujących zagrożeń,
   b) powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, utratą, uszkodzeniem lub zniszczeniem,
   c) dopuszczać do przetwarzana danych wyłącznie osoby, które zobowiązały się do zachowania tajemnicy lub podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy.
2. Podmiot przetwarzający zobowiązuje się do przetwarzania danych osobowych wyłącznie na udokumentowane polecenie Administratora.
3. Podmiot przetwarzający zobowiązany jest do zgłaszania Administratorowi przypadków naruszeń ochrony danych osobowych w ciągu 24 godzin od stwierdzenia naruszenia.

§ 4

Oświadczenie Podmiotu przetwarzającego

1. Zobowiązuję się do wykorzystania powierzonych danych osobowych wyłącznie w zakresie i celu niezbędnym do realizacji obowiązków wynikających z umowy współpracy.
2. W przypadku ogólnej pisemnej zgody na korzystanie z usług innego podmiotu przetwarzającego poinformuję Administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających.
3. W miarę możliwości będę pomagać Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw.
4. W przypadku audytów lub inspekcji przeprowadzonych lub zleconych przez Administratora udostępnię wszelkie niezbędne informacje z zachowaniem czujności, czy żądane informacje nie naruszą zapisów Rozporządzenia.

§ 5

Zakres odpowiedzialności

1. Każda ze Stron odpowiada za szkody wyrządzone drugiej Stronie oraz osobom trzecim w związku z wykonywaniem niniejszej Umowy, zgodnie z przepisami Rozporządzenia i Kodeksu cywilnego.
2. W celu uniknięcia wątpliwości, Podmiot przetwarzający ponosi odpowiedzialność za działania swoich pracowników i innych osób, przy pomocy których przetwarza powierzone dane osobowe, jak za własne działanie i zaniechanie.

§ 6

Czas trwania i wypowiedzenie Umowy

1. Umowa zostaje zawarta na czas obowiązywania Umowy głównej. W celu uniknięcia wątpliwości, rozwiązanie Umowy głównej skutkuje rozwiązaniem niniejszej Umowy.
2. Strony postanawiają, iż po zakończeniu przetwarzania danych Podmiot powierzający zobowiązany jest do niezwłocznego usunięcia powierzonych mu danych (i wszelkich ich istniejących kopii) lub zwrotu Administratorowi – w zależności od jego decyzji, o ile nie następuje konieczność dalszego przetwarzania danych wynikająca z przepisów odrębnych.
3. Administrator jest uprawniony do rozwiązania Umowy bez wypowiedzenia, jeżeli Podmiot przetwarzający nie podjął środków zabezpieczających powierzone dane lub nie stosował się do wymogów przewidzianych w Rozporządzeniu.
4. Każdej ze Stron przysługuje prawo rozwiązania niniejszej Umowy w trybie natychmiastowym, w przypadku naruszenia postanowień niniejszej Umowy przez drugą Stronę Umowy.

§ 7

Postanowienia końcowe

1. Z tytułu wykonywania świadczeń określonych w niniejszej Umowie Podmiotowi przetwarzającemu nie przysługuje dodatkowe wynagrodzenie ponad to, które zostało określone w Umowie głównej.
2. Umowa wchodzi w życie z dniem jej podpisania przez Strony.
3. W sprawach nieuregulowanych niniejszą Umową zastosowanie mają powszechnie obowiązujące przepisy prawa polskiego.
4. Wszelkie zmiany lub uzupełnienia niniejszej Umowy wymagają zachowania formy pisemnej pod rygorem nieważności.
5. Sądem właściwym dla rozstrzygania sporów powstałych w związku z realizacją niniejszej Umowy jest sąd właściwy dla siedziby Administratora.
6. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

Podpisy:

……..… ……..

Administrator *Podmiot przetwarzający*

załącznik nr 7

Wykaz podmiotów, którym powierzono przetwarzanie danych

Lp.	Nazwa podmiotu	Data zawarcia umowy powierzenia
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		

załącznik nr 8

Wykaz wprowadzonych zabezpieczeń

ORGANIZACYJNE	1.	Sporządzono i wdrożono dokumenty uzupełniające ogólną politykę, regulujące zasady przetwarzania i zabezpieczania danych osobowych.
	2.	Do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez Administratora.
	3.	Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego.
	4.	Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy.
	5.	Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych.
	6.	Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych.
	7.	Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych.
	8.	Wprowadzono zasadę „czystego biurka", „czystego ekranu", „białej kartki".
	9.	Dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonując takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści, aby po dokonaniu usunięcia danych niemożliwa była identyfikacja osób.
	10.	Informacji telefonicznych nie udziela się, względnie udziela się po zidentyfikowaniu rozmówcy i stwierdzeniu jego upoważnienia do uzyskania danych.
	11.	Powołano Inspektora ds. bezpieczeństwa IT w związku z wymogami Ustawy z dnia 5.VII 2018r. w krajowym systemie cyberbezpieczeństwa.

FIZYCZNE	1.	Urządzenia służące do przetwarzania danych osobowych umieszcza się w zamykanych biurkach i szafach.
	2.	Pomieszczenia, w których przechowywane są dane osobowe zamykane są na klucz.
	3.	Dokumentacja zabezpieczona w zamykanych szafach metalowych i niemetalowych.
	4.	Firma ochroniarska – całodobowa ochrona obiektu.

TECHNICZNE	1.	Na każdej stacji roboczej jest rozbudowany program antywirusowy wraz z Firewall połączony centralnym serwerem zarządzającym Managment Server G Data.
	2.	Stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową.
	3.	Konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych przechowywanych w systemie informatycznym wyłącznie za pośrednictwem używanych aplikacji.
	4.	Komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych, za pomocą indywidualnego identyfikatora użytkowania i hasła.
	5.	Zastosowano UPS (w serwerowni)

załącznik nr 9

Raport z naruszenia bezpieczeństwa danych osobowych

Nr raportu ..... /.....

Data wystąpienia zdarzenia ..... godzina .....

Miejsce wystąpienia zdarzenia .....

Osoba zawiadamiająca .....

Opis zdarzenia i rodzaj naruszenia

.....
.....
.....
.....

Przyczyny powstania zdarzenia

.....
.....
.....
.....

Zaistniałe skutki zagrożenia

.....
.....
.....
.....

Podjęte czynności naprawczo-zapobiegawcze

.....
.....
.....
.....

Osoby zaangażowane w wyjaśnienie zdarzenia

.....
.....

Zdarzenie skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych TAK NIE *****

Podpisy:

....

Osoba nadzorująca *Osoba zgłaszająca*

* właściwe podkreślić

załącznik nr 10

Wykaz osób zapoznanych z zapisami dokumentacji z ochrony danych osobowych

Lp.	Imię i nazwisko	Data zapoznania	Podpis
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			

Lp.	Imię i nazwisko	Data zapoznania	Podpis

Załącznik nr 11

Wniosek o sprostowanie danych osobowych

Dane Wnioskodawcy *(osoby, której dane dotyczą)*

Imię i nazwisko: …….
Adres zamieszkania: …….
Numer klienta: ……..
Zwracam się z prośbą o sprostowanie moich następujących danych osobowych: *(zaznacz właściwe pola i podaj obok nowe poprawne dane)*

- ☐ Imię: ……
- ☐ Nazwisko: ……
- ☐ Adres zameldowania: ……..
- ☐ Adres zamieszkania: ……
- ☐ Adres do korespondencji: ……..
- ☐ Telefon komórkowy: ……
- ☐ Inne *(prosimy podać jakie)*: …….

Oświadczam, że powyżej wskazane dane zgodne są ze stanem faktycznym.
Przyjmuję do wiadomości, że wniosek będzie skuteczny dopiero po zweryfikowaniu mojej tożsamości.

INFORMACJA DOTYCZACA OCHRONY DANYCH OSOBOWYCH.
Na podstawie Rozporządzenia 2016/679 Parlamentu Europejskiego i Rady Unii Europejskiej z dnia 27 kwietnia 2016 roku oraz uchylenia dyrektywy 95/46/WE, oraz w związku z wejściem w życie ustawy z dnia 10 maja 2018 o ochronie danych osobowych, informujemy, iż przysługują Państwu określone poniżej prawa związane z przetwarzaniem danych osobowych:

1. Administratorem Państwa danych osobowych jest Pyrzyckie Przedsiębiorstwo Komunalne Sp. z .o.o. w Pyrzycach z siedzibą w Pyrzycach przy ul. Kościuszki 26. Pyrzyckie Przedsiębiorstwo Komunalne Sp. z o.o. wyznaczyło inspektora ochrony danych osobowych, którym jest Pani Karolina Chiciak. Kontakt: chiciak.k@ppkpyrzyce.pl, telefon: 91 579 19 62.
2. Państwa dane osobowe będą przetwarzane w następujących celach: w celu złożenia wniosku o sprostowanie danych osobowych.
3. Państwa dane osobowe są pozyskiwane w zakresie niezbędnym do złożenia wniosku. Po tym okresie dane będą przetwarzane jedynie w zakresie i przez czas wymagany przepisami prawa. Konsekwencją nie podania wymaganych danych jest brak możliwości złożenia wniosku.
4. Państwa dane osobowe mogą być przekazywane podmiotom świadczącym działalność pocztową i kurierską, bankom w zakresie realizacji płatności, organom uprawnionym do otrzymania Państwa danych osobowych na podstawie przepisów prawa, podmiotom obsługującym nasze systemy teleinformatyczne, podmiotom działającym na nasze zlecenie, np. świadczące pomoc prawną. Państwa dane osobowe nie będą podlegały profilowaniu.
5. Przysługuje Państwu prawo dostępu do treści przetwarzanych danych, wycofania zgody na przetwarzanie, żądania ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo przenoszenia danych oraz prawo wniesienia sprzeciwu względem przetwarzanych danych osobowych.
6. Przysługuje Państwu prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych.

…….. ……
Data i miejscowość *Podpis*

Tożsamość Wnioskodawcy została zweryfikowana pozytywnie.
…….....
Data i podpis

Załącznik nr 12

Wniosek o usunięcie danych osobowych

Dane Wnioskodawcy *(osoby, której dane dotyczą)*

Imię i nazwisko: ……

Adres zamieszkania: ……..

Nr klienta: ……..

Zwracam się z prośbą o usunięcie moich danych osobowych, powołując się na fakt, że nie istnieją podstawy prawne do ich przetwarzania.
Przyjmuję do wiadomości, że wniosek będzie skuteczny dopiero po zweryfikowaniu mojej tożsamości.

…….. ……

Data i miejscowość *Podpis*

INFORMACJA DOTYCZACA OCHRONY DANYCH OSOBOWYCH.

Na podstawie Rozporządzenia 2016/679 Parlamentu Europejskiego i Rady Unii Europejskiej z dnia 27 kwietnia 2016 roku oraz uchylenia dyrektywy 95/46/WE, oraz w związku z wejściem w życie ustawy z dnia 10 maja 2018 o ochronie danych osobowych, informujemy, iż przysługują Państwu określone poniżej prawa związane z przetwarzaniem danych osobowych:

1. Administratorem Państwa danych osobowych jest Pyrzyckie Przedsiębiorstwo Komunalne Sp. z .o.o. w Pyrzycach z siedzibą w Pyrzycach przy ul. Kościuszki 26. Pyrzyckie Przedsiębiorstwo Komunalne Sp. z o.o. wyznaczyło inspektora ochrony danych osobowych, którym jest Pani Karolina Chiciak. Kontakt: chiciak.k@ppkpyrzyce.pl, telefon: 91 579 19 62
2. Państwa dane osobowe będą przetwarzane w następujących celach: w celu złożenia wniosku o usunięcie danych osobowych.
3. Państwa dane osobowe są pozyskiwane w zakresie niezbędnym do złożenia wniosku. Po tym okresie dane będą przetwarzane jedynie w zakresie i przez czas wymagany przepisami prawa. Konsekwencją nie podania wymaganych danych jest brak możliwości złożenia wniosku.
4. Państwa dane osobowe mogą być przekazywane podmiotom świadczącym działalność pocztową i kurierską, bankom w zakresie realizacji płatności, organom uprawnionym do otrzymania Państwa danych osobowych na podstawie przepisów prawa, podmiotom obsługującym nasze systemy teleinformatyczne, podmiotom działającym na nasze zlecenie, np. świadczące pomoc prawną. Państwa dane osobowe nie będą podlegały profilowaniu.
5. Przysługuje Państwu prawo dostępu do treści przetwarzanych danych, wycofania zgody na przetwarzanie, żądania ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo przenoszenia danych oraz prawo wniesienia sprzeciwu względem przetwarzanych danych osobowych.
6. Przysługuje Państwu prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych.

Tożsamość Wnioskodawcy została zweryfikowana pozytywnie.

……....

Data i podpis

Załącznik nr 13.

Wniosek o ograniczenie przetwarzania danych osobowych

Dane Wnioskodawcy *(osoby, której dane dotyczą)*

Imię i nazwisko: ……
Adres zamieszkania: …….
Nr klienta: ……
Zwracam się z prośbą o: *(zaznacz właściwe pola)*

- wstrzymanie operacji na moich danych osobowych ze względu na:
  - ☐ nieprawidłowość danych osobowych (na okres sprawdzenia ich poprawności)
  - ☐ niezgodność przetwarzania z prawem *(możesz domagać się ich usunięcia)*
  - ☐ wniesiony sprzeciw (do czasu jego rozstrzygnięcia)
- nieusuwanie moich danych osobowych, ponieważ:
  - ☐ potrzebuję wykorzystać je do ustalenia/dochodzenia/obrony roszczeń (w sytuacji, gdy administrator nie potrzebuje już danych osobowych do celów przetwarzania)

Przyjmuję do wiadomości, że wniosek będzie skuteczny dopiero po zweryfikowaniu mojej tożsamości.

INFORMACJA DOTYCZACA OCHRONY DANYCH OSOBOWYCH.

Na podstawie Rozporządzenia 2016/679 Parlamentu Europejskiego i Rady Unii Europejskiej z dnia 27 kwietnia 2016 roku oraz uchylenia dyrektywy 95/46/WE, oraz w związku z wejściem w życie ustawy z dnia 10 maja 2018 o ochronie danych osobowych, informujemy, iż przysługują Państwu określone poniżej prawa związane z przetwarzaniem danych osobowych:

1. Administratorem Państwa danych osobowych jest Pyrzyckie Przedsiębiorstwo Komunalne Sp. z .o.o. w Pyrzycach z siedzibą w Pyrzycach przy ul. Kościuszki 26. Pyrzyckie Przedsiębiorstwo Komunalne Sp. z o.o. wyznaczyło inspektora ochrony danych osobowych, którym jest Pani Karolina Chiciak. Kontakt: chiciak.k@ppkpyrzyce.pl, telefon: 91 579 19 62
2. Państwa dane osobowe będą przetwarzane w następujących celach: w celu złożenia wniosku o ograniczenie przetwarzania danych osobowych.
3. Państwa dane osobowe są pozyskiwane w zakresie niezbędnym do złożenia wniosku. Po tym okresie dane będą przetwarzane jedynie w zakresie i przez czas wymagany przepisami prawa. Konsekwencją nie podania wymaganych danych jest brak możliwości złożenia wniosku.
4. Państwa dane osobowe mogą być przekazywane podmiotom świadczącym działalność pocztową i kurierską, bankom w zakresie realizacji płatności, organom uprawnionym do otrzymania Państwa danych osobowych na podstawie przepisów prawa, podmiotom obsługującym nasze systemy teleinformatyczne, podmiotom działającym na nasze zlecenie, np. świadczące pomoc prawną. Państwa dane osobowe nie będą podlegały profilowaniu.
5. Przysługuje Państwu prawo dostępu do treści przetwarzanych danych, wycofania zgody na przetwarzanie, żądania ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo przenoszenia danych oraz prawo wniesienia sprzeciwu względem przetwarzanych danych osobowych.
6. Przysługuje Państwu prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych.

…….. ……
Data i miejscowość *Podpis*

Tożsamość Wnioskodawcy została zweryfikowana pozytywnie.

…….....
Data i podpis

Załącznik nr 14

Wniosek o przeniesienie danych osobowych

Dane Wnioskodawcy *(osoby, której dane dotyczą)*

Imię i nazwisko: …….
Adres zamieszkania: …….
Numer klienta: ……..
Zwracam się z prośbą o przeniesienie moich danych osobowych.
Oświadczenie Wnioskodawcy w sprawie formy przekazania danych osobowych Wnioskodawcy lub innemu administratorowi:
……
……
……

Oświadczam, że powyżej wskazane dane zgodne są ze stanem faktycznym.
Przyjmuję do wiadomości, że wniosek będzie skuteczny dopiero po zweryfikowaniu mojej tożsamości.

INFORMACJA DOTYCZACA OCHRONY DANYCH OSOBOWYCH.
Na podstawie Rozporządzenia 2016/679 Parlamentu Europejskiego i Rady Unii Europejskiej z dnia 27 kwietnia 2016 roku oraz uchylenia dyrektywy 95/46/WE, oraz w związku z wejściem w życie ustawy z dnia 10 maja 2018 o ochronie danych osobowych, informujemy, iż przysługują Państwu określone poniżej prawa związane z przetwarzaniem danych osobowych:

7. Administratorem Państwa danych osobowych jest Pyrzyckie Przedsiębiorstwo Komunalne Sp. z .o.o. w Pyrzycach z siedzibą w Pyrzycach przy ul. Kościuszki 26. Pyrzyckie Przedsiębiorstwo Komunalne Sp. z o.o. wyznaczyło inspektora ochrony danych osobowych, którym jest Pani Karolina Chiciak. Kontakt: chiciak.k@ppkpyrzyce.pl, telefon: 91 579 19 62.
8. Państwa dane osobowe będą przetwarzane w następujących celach: w celu złożenia wniosku o przeniesienie danych osobowych.
9. Państwa dane osobowe są pozyskiwane w zakresie niezbędnym do złożenia wniosku. Po tym okresie dane będą przetwarzane jedynie w zakresie i przez czas wymagany przepisami prawa. Konsekwencją nie podania wymaganych danych jest brak możliwości złożenia wniosku.
10. Państwa dane osobowe mogą być przekazywane podmiotom świadczącym działalność pocztową i kurierską, bankom w zakresie realizacji płatności, organom uprawnionym do otrzymania Państwa danych osobowych na podstawie przepisów prawa, podmiotom obsługującym nasze systemy teleinformatyczne, podmiotom działającym na nasze zlecenie, np. świadczące pomoc prawną. Państwa dane osobowe nie będą podlegały profilowaniu.
11. Przysługuje Państwu prawo dostępu do treści przetwarzanych danych, wycofania zgody na przetwarzanie, żądania ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo przenoszenia danych oraz prawo wniesienia sprzeciwu względem przetwarzanych danych osobowych.
12. Przysługuje Państwu prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych.

…….. ……
Data i miejscowość *Podpis*

Tożsamość Wnioskodawcy została zweryfikowana pozytywnie.
…….....
Data i podpis

Informacja na temat technicznej możliwości przekazania danych:
……
……