POLITYKA

OCHRONY DANYCH OSOBOWYCH

W SPÓŁCE:

„AGRECO SERVICE”
SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

WERSJA DOKUMENTU:	**1.0**
WESZŁA W ŻYCIE:	**25.05.2018 r.**
TERMIN NASTĘPNEJ WERYFIKACJI:	**25.05.2020 r.**

DZIAŁ I: ZASADY

I. CEL POLITYKI OCHRONY DANYCH OSOBOWYCH

1. Polityka Ochrony Danych Osobowych została utworzona w związku z wymaganiami zawartymi w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – dalej: „**RODO**".

2. Określa się następujące definicje najważniejszych pojęć użytych w niniejszym dokumencie:

   a) **Polityka** lub **PODO** – niniejsza Polityka Ochrony Danych Osobowych.

   b) **Przedsiębiorstwo** – rozumie się przez to „AGRECO SERVICE" Sp. z o.o. z siedzibą w Kostrzynie nad Odrą, ul. Prosta 3, 5, 7, 66-470 Kostrzyn nad Odrą, wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego pod numerem KRS 0000248395, NIP nr 5993070616, REGON nr 080076104.

   c) **Dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

   d) **Przetwarzanie** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

   e) **Zbiór danych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

II. PODSTAWOWE ZASADY

Przedsiębiorstwo wdraża niniejszą Politykę, aby zapewnić, że dane osobowe przekazane do przetwarzania przez Przedsiębiorstwo będą:

a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
b) zbierane w konkretnych, wyraźnych i uzasadnionych celach oraz nieprzetwarzane dalej w sposób niezgodny z tymi celami;
c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
d) prawidłowe i w razie potrzeby uaktualniane;
e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane;
f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

III. ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH

1. Przetwarzanie danych osobowych przez Przedsiębiorstwo w podstawowym zakresie odbywa się na podstawie zgody osoby, której dane dotyczą.
2. Zgoda może być udzielona zarówno pisemnie, jak i za pośrednictwem środków porozumiewania się na odległość.
3. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Jednakże wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.
4. Zgoda na przetwarzanie danych osobowych może być udzielona jedynie przez osobę, która ukończyła 18 rok życia. W imieniu osób poniżej tej granicy wieku, zgoda musi być wyrażona przez przedstawicieli ustawowych tej osoby.

IV. POZOSTAŁE PODSTAWY PRZETWARZANIA DANYCH OSOBOWYCH

Przedsiębiorstwo może przetwarzać dane osobowe także, gdy:

a) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
b) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Przedsiębiorstwie;
c) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
d) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Przedsiębiorstwu;

e) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Przedsiębiorstwo lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

V. DOSTĘP DO DANYCH OSOBOWYCH

1. Osoba, której dotyczą dane osobowe, jest uprawniona do uzyskania od Przedsiębiorstwa potwierdzenia, czy przetwarzane są przez Przedsiębiorstwo dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:
    a) cele przetwarzania;
    b) kategorie odnośnych danych osobowych;
    c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
    d) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
    e) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
    f) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
2. Na zgłoszone żądanie, Przedsiębiorstwo dostarczy osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, Przedsiębiorstwo może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych.
3. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.

VI. SPROSTOWANIE DANYCH OSOBOWYCH

Osoba, której dane dotyczą, ma prawo żądania niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

VII. USUNIĘCIE DANYCH OSOBOWYCH („BYCIE ZAPOMNIANYM")

1. Osoba, której dane dotyczą, ma prawo żądania niezwłocznego usunięcia dotyczących jej danych osobowych, a Przedsiębiorstwo bez zbędnej zwłoki usunie dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;
c) osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania;
d) dane osobowe były przetwarzane niezgodnie z prawem;
e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii Europejskiej lub prawie polskim;
f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.

2. W przypadku gdy Przedsiębiorstwo dokonało upublicznienia danych osobowych, a ma obowiązek usunąć te dane zgodnie z postanowieniem powyżej, to – biorąc pod uwagę dostępną technologię i koszt realizacji – Przedsiębiorstwo podejmuje rozsądne działania, w tym środki techniczne, by poinformować wszystkich innych administratorów przetwarzających takie dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.
3. Przedsiębiorstwo będzie miało prawo odmówić usunięcia w całości lub części danych osobowych, jeżeli ich przetwarzanie jest niezbędne:
    a) do korzystania z prawa do wolności wypowiedzi i informacji;
    b) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa, któremu podlega Przedsiębiorstwo;
    c) do ustalenia, dochodzenia lub obrony roszczeń.

DZIAŁ II: KWESTIE PODSTAWOWE

1. OSOBY ZAANGAŻOWANE W PROCES PRZETWARZANIA DANYCH OSOBOWYCH

1.1. Administrator danych osobowych

Administratorem danych osobowych jest Przedsiębiorstwo.
Działania Przedsiębiorstwa jako administratora wykonuje Zarząd Przedsiębiorstwa wedle uprawnień do jego reprezentacji na zewnątrz.

1.2. Zbiory danych osobowych

Przedsiębiorstwo dokonuje podziału posiadanych i przetwarzanych danych osobowych na zbiory, które utworzone są w oparciu o cechę kluczową osób, których dany zbiór dotyczy, lub zawartości tego zbioru, lub sposobu pozyskiwania danych do danego zbioru.

Jednie osoby upoważnione do przetwarzania danego zbioru mogą mieć do niego dostęp.

Lista zbiorów danych osobowych stanowi **załącznik nr 1** do Polityki.

1.3. Osoby upoważnione do przetwarzania danych osobowych

Przedsiębiorstwo prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych ze wskazaniem celów konkretnego upoważnienia oraz zbiorów danych osobowych, których dotyczy upoważnienie.

Ewidencja osób upoważnionych do przetwarzania danych osobowych prowadzona jest w formie pisemnej oraz może być prowadzona także w formie elektronicznej.
Forma pisemna stanowi **załącznik nr 2** do Polityki.

Upoważnienia nadaje oraz cofa się w formie pisemnej.
Wzór upoważnienia stanowi **załącznik nr 3** do Polityki.

Każda osoba upoważniona do przetwarzania danych osobowych musi zostać zobowiązana do zachowania ich w ścisłej tajemnicy na piśmie.
Wzór oświadczenia osoby upoważnionej stanowi **załącznik nr 4** do Polityki.

1.4. Podmioty przetwarzające

Przedsiębiorstwo może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej lub elektronicznej, zgodnie z wymogami wskazanymi dla takich umów w art. 28 RODO.

Przed powierzeniem przetwarzania danych osobowych Przedsiębiorstwo w miarę możliwości uzyskuje informacje o dotychczasowych praktykach podmiotu przetwarzającego dotyczących zabezpieczenia danych osobowych.

Wykaz podmiotów przetwarzających, z którymi jest prowadzona współpraca stanowi **załącznik nr 5** do Polityki.

2. RODZAJE PRZETWARZANYCH DANYCH OSOBOWYCH

Przedsiębiorstwo, różnych sytuacjach, przetwarza lub może przetwarzać następujące rodzaje danych osobowych:

a) Imię i nazwisko,
b) Adres zamieszkania, adres zameldowania, adres korespondencyjny,
c) Numer identyfikacyjny (NIP, PESEL);
d) Numer dowodu osobistego;
e) Dane kontaktowe: numery telefonów, e-maile, wizytówki;
f) Ograniczone dane finansowe – numer konta bankowego, bank;
g) Ograniczone dane o stanie zdrowia;
h) Ograniczone dane o poziomie niepełnosprawności;
i) Dane zawarte w dokumentach przekazywanych do zniszczenia;
j) Adresy IP.

Nie jest wykluczone przetwarzanie innych danych, niż tylko te, które zostały wskazane powyżej, lecz każdorazowo musi się to odbywać albo na podstawie zgody, o której mowa w Dziale I punkt III lub na jednej z pozostałych podstaw wskazanych w Dziale I punkt IV.

Ponadto, Przedsiębiorstwo na cele przyszłej umowy lub zawartej już umowy, może pobierać dane osobowe o charakterze szczególnym, dotyczących stanu zdrowia – na cele zawarcia umowy o pracę lub podobnej. W takim przypadku, przed przystąpieniem do pobrania i przetwarzania tego rodzaju danych, Przedsiębiorstwo będzie obowiązane zawsze uzyskać zgodę osoby, której to dotyczy, zgodnie z art. 9 ust. 2 lit. a) RODO.

3. NOŚNIKI DANYCH OSOBOWYCH I SYSTEMY INFORMATYCZNE

W ramach przetwarzania danych osobowych Przedsiębiorstwo będzie wykorzystywać następujące nośniki danych:

a) Dokumentacja papierowa;
b) Dyski twarde;
c) Telefony komórkowe;
d) Pendrive'y;
e) Płyty DVD/CD.

Systemy informatyczne i programy komputerowe, które są wykorzystywane, lub będą wykorzystywane:

a) Internetowe skrzynki pocztowe;
b) Aplikacje web.
c) Pakiety biurowe.

4. POMIESZCZENIA, W KTÓRYCH SĄ PRZETWARZANE DANE OSOBOWE

4.1. Pomieszczenia

W zakresie zabezpieczenia organizacyjnego i technicznego niniejsza Polityka dotyczy siedziby Przedsiębiorstwa i wszelkich nieruchomości znajdujących się pod bezpośrednią kontrolą Przedsiębiorstwa – placówek handlowych, filii, oddziałów, biur terenowych itp.

Zasady zarządzania pomieszczeniami w zakresie danych osobowych są następujące:

1) Pomieszczenia, w których znajdują się przetwarzane zbiory danych osobowych, muszą pozostawać pod osobistym nadzorem upoważnionych do ich przetwarzania osób.
2) Dane osobowe są gromadzone, przechowywane i przetwarzane w kartotekach, skorowidzach, księgach, wykazach oraz w innych podobnych zbiorach.
3) Opuszczenie pomieszczenia, w których znajdują się jakiekolwiek zbiory danych osobowych musi być poprzedzone przeniesieniem zbioru danych do odpowiednio zabezpieczonego miejsca, zamykanego na klucz (szafa, skrytka, szuflada itp.).
4) Przy planowanej nieobecności osoby, pod nadzorem której pozostaje pomieszczenie, samo pomieszczenie powinno być zamknięte na klucz.
5) Klucze do szaf, w których przechowywane są dane osobowe mają jedynie osoby upoważnione do przetwarzania danych osobowych.

4.2. Monitoring

Zarówno budynki, ich najbliższe otoczenie oraz wewnętrzne części wspólne (z wyłączeniem łazienek i toalet) mogą być objęte monitoringiem audio-wizualnym.

Zasady prowadzenia monitoringu audio-wizualnego są następujące:

1) W zakresie dotyczącym monitoringu obejmującego osoby zatrudnione przez Przedsiębiorstwo – Przedsiębiorstwo podaje informacje o takim monitoringu swojej załodze w sposób zwyczajowo przyjęty. Nie dotyczy to monitoringu istniejącego przed wejściem w życie niniejszej Polityki.
2) Zapis z monitoringu może być przechowywany przez 30 dni od jego wykonania.
3) Pomieszczenia lub otoczenie budynków objęte monitoringiem musi być oznaczone w widocznym miejscu informacją o tym, iż prowadzony jest monitoring.

4.3. Klucze

Przedsiębiorstwo wdrożyło zasady zarządzania kluczami wewnętrznymi, które mają na celu ograniczenie dostępności jedynie do upoważnionych osób.

Klucze wydaje oraz zarządza nimi Administrator lub upoważniona przez niego osoba.

4.4. Zasada czystego biurka

Każda osoba upoważniona do przetwarzania danych osobowych:

1) zobowiązana jest do przechowywania na biurku tylko tych dokumentów, które są potrzebne do wykonywania w danym momencie pracy;
2) dokumenty wykorzystywane do pracy nie mogą być położone w taki sposób, aby nieupoważniona osoba trzecia mogła zapoznać się choćby z fragmentem ich treści;
3) nie może przetrzymywać na biurku jedzenia oraz picia;
4) po zakończonej pracy zobowiązana jest do zabezpieczenia dokumentów w odpowiednim miejscu, w tym także jeżeli jest to wymagane to w zamykanej na klucz szafie lub skrytce;
5) zobowiązana jest do niszczenia dokumentów niepotrzebnych w taki sposób, aby nie było możliwe odtworzenie zawartych w nich informacji, np. w niszczarce.

4.5. Zasady ustawienia monitorów

Każdy monitor komputerowy musi być ustawiony, aby spełniał następujące warunki:

1) ustawienie monitora musi być takie, aby wykluczyć lub w maksymalnym stopniu zmniejszać możliwość odczytania wyświetlanych na nich informacji przez nieupoważnioną osobę trzecią;
2) użytkownik komputera powinien blokować lub zmieniać obraz wyświetlany na monitorze na neutralny za każdym razem, gdy nieupoważniona osoba trzecia mogłaby zobaczyć wyświetlane na monitorze informacje;
3) każdy komputer musi mieć ustawiony wygaszacz ekrany uruchamiający się po min. 5 minutach bezczynności, a którego wyłączenie wymaga autoryzacji hasłem;
4) opuszczenie pomieszczenia, w których znajdują się komputery z monitorami musi być poprzedzone albo wyłączeniem komputera albo dokonaniem takiej jego blokady, aby wznowienie pracy wymagało autoryzacji hasłem.

5. METODY POZYSKIWANIA DANYCH OSOBOWYCH

5.1. Telefoniczna

W przypadku, gdy dane osobowe pozyskiwane są za pośrednictwem telefonu, prowadzący rozmowę przedstawiciel Przedsiębiorstwa jest obowiązany:

1) we wstępnej części rozmowy poinformować o tym, że na cele przyszłej współpracy i zawarcia umowy konieczne jest pobranie oraz przetworzenie danych osobowych,
2) wskazać jakie dane osobowe będą niezbędne celem zawarcia umowy,
3) uzyskać werbalną zgodę na przetwarzanie danych osobowych,
4) przy kolejnym kontakcie z osobą, której dane dotyczą, w formie innej niż telefoniczna, np. osobistej, elektronicznej lub listownej – doręczyć kartę informacyjną, o której mowa w punkcie 6 niniejszej Polityki.

Jeżeli osoba, z którą przedstawiciel Przedsiębiorstwa toczy rozmowę telefoniczną, wyrazi werbalną zgodę na przetwarzanie danych osobowych, to współpraca może być nawiązana.

Jeżeli zgoda na przetwarzanie danych osobowych nie zostanie udzielona werbalnie, to współpraca nie może być nawiązana, a przedstawiciel Przedsiębiorstwa jest obowiązany zakończyć rozmowę telefoniczną. W takim przypadku żadne dane osobowe rozmówcy nie zostają nigdzie utrwalone i nie będą więcej przetwarzane w żadnej formie.

Rozmowy telefoniczne co do zasady nie są rejestrowane. W przypadku odstępstwa od tej zasady, przedstawiciel Przedsiębiorstwa jest obowiązany poinformować swojego rozmówcę na samym początku połączenia o tym, iż rozmowa jest rejestrowana i jej kontynuowanie oznacza zgodę na rejestrację.

5.2. Elektroniczna (w szczególności: e-mail)

W przypadku, gdy dane osobowe pozyskiwane są za pośrednictwem środków komunikacji elektronicznej, w szczególności za pomocą e-maili, wiadomości tekstowych, komunikatorów internetowych itp., to używający danej metody komunikacji przedstawiciel Przedsiębiorstwa jest obowiązany:

1) przy pierwszej możliwej okazji powiadomić osobę, której dane osobowe mają być przetwarzane, o konieczności pobrania i przetwarzania danych osobowych na cele przyszłej współpracy i zawarcia umowy,
2) wskazać jakie dane osobowe będą niezbędne celem zawarcia umowy,
3) uzyskać w danej formie elektronicznej zgodę na przetwarzanie danych osobowych,
4) przekazać w danej formie elektronicznej kartę informacyjną, o której mowa w punkcie 6 niniejszej Polityki.

Jeżeli osoba, z którą przedstawiciel Przedsiębiorstwa toczy rozmowę drogą elektroniczną, wyrazi w tej formie zgodę na przetwarzanie danych osobowych, to współpraca może być nawiązana.

Jeżeli zgoda na przetwarzanie danych osobowych nie zostanie udzielona w danej formie, to współpraca nie może być nawiązana, a przedstawiciel Przedsiębiorstwa jest obowiązany usunąć wszelkie dane osobowe, które mogły zostać do tej pory pobrane.

5.3. Osobista

W przypadku, gdy dane osobowe pozyskiwane są osobiście, np. w siedzibie Przedsiębiorstwa, to przedstawiciel Przedsiębiorstwa jest obowiązany:

1) ustnie powiadomić osobę, której dane osobowe mają być przetwarzane, o konieczności pobrania i przetwarzania danych osobowych na cele przyszłej współpracy i zawarcia umowy,
2) wskazać jakie dane osobowe będą niezbędne celem zawarcia umowy,
3) uzyskać ustną zgodę na przetwarzanie danych osobowych,
4) przekazać na piśmie kartę informacyjną, o której mowa w punkcie 6 niniejszej Polityki.

Jeżeli osoba, z którą przedstawiciel Przedsiębiorstwa toczy rozmowę, wyrazi zgodę na przetwarzanie danych osobowych, to współpraca może być nawiązana.

Jeżeli zgoda na przetwarzanie danych osobowych nie zostanie udzielona, to współpraca nie może być nawiązana, a przedstawiciel Przedsiębiorstwa jest obowiązany zwrócić wszelkie nośniki danych osobowych, które mógł do tej pory otrzymać.

5.4. Korespondencyjna

W przypadku, gdy dane osobowe pozyskiwane są za pośrednictwem korespondencji pocztowej, to używający tej metody komunikacji przedstawiciel Przedsiębiorstwa jest obowiązany:

1) zapewnić, że wysyłane dokumenty zawierają w sobie informacje o koniecznych do pobrania i przetwarzania danych osobowych na cele przyszłej współpracy i zawarcia umowy – co może mieć postać odpowiednich klauzul umownych,
2) zapewnić, że wysyłane dokumenty zawierają możliwość wyrażenia zgody na przetwarzanie danych osobowych – co może mieć postać odpowiedniej klauzuli umownej,
3) załączyć w do korespondencji kartę informacyjną, o której mowa w punkcie 6 niniejszej Polityki.

Jeżeli osoba, do której przedstawiciel Przedsiębiorstwa przesłał korespondencję pocztową odpowie w tej samej formie i w odpowiedni sposób wyrazi zgodę na przetwarzanie danych osobowych, to współpraca może być nawiązana.

Jeżeli osoba, do której przedstawiciel Przedsiębiorstwa przesłał korespondencję pocztową nie odpowie na tę korespondencję w żaden sposób w ciągu 30 dni od wysłania, domniemuje się że nie udzieliła ona zgody na przetwarzanie danych osobowych. W konsekwencji współpraca nie może być nawiązana, a przedstawiciel Przedsiębiorstwa jest obowiązany usunąć wszelkie dane osobowe, które mogły zostać do tej pory pobrane. To samo dotyczy sytuacji, w której osoba, której to dotyczy, oświadczyła w dowolnej formie w odpowiedzi na otrzymaną korespondencję, iż nie wyraża zgody na przetwarzanie jej danych osobowych.

6. NISZCZENIE NOŚNIKÓW DANYCH OSOBOWYCH

Przedsiębiorstwo zajmuje się profesjonalnie m.in. niszczeniem i utylizacją nośników zawierających dane osobowe.

W tym celu Przedsiębiorstwo będzie zawierać z każdym zainteresowanym klientem szczególną umowę powierzenia przetwarzania nośników zawierających dane osobowe – na cele ich zniszczenia. Umowa ta będzie w sposób szczegółowy opisywać rodzaje, zasady i sposoby niszczenia przekazywanych nośników, tak aby niemożliwe było odczytanie z nich jakichkolwiek danych osobowych.

7. KARTA INFORMACYJNA

Przedsiębiorstwo wypełnia wszelkie obowiązki informacyjne dotyczące przetwarzania danych osobowych określone w art. 13 i 14 RODO poprzez przekazywanie osobą, których to dotyczy, ustandaryzowanych kart informacyjnych.

Doręczenie karty informacyjnej może nastąpić zarówno osobiście, drogą elektroniczną jak i korespondencją pocztową – w zależności od wybranej formy kontaktu.

Wzór karty informacyjnej obowiązującej na dzień ostatniej aktualizacji niniejszej Polityki stanowi załącznik nr 7.

DZIAŁ III: PRACOWNICY

Niniejszy dział poświęcony jest szczególnym zasadom przetwarzania danych osobowych pracowników. W zakresie nieuregulowanym postanowienia Działów I i II Polityki mają odpowiednie zastosowanie.

1. Rodzaje danych osobowych pracowników

Przedsiębiorstwo przetwarza lub może przetwarzać następujące rodzaje danych osobowych pracowników:

a) imię i nazwisko;
b) dane teleadresowe;
c) numer identyfikacyjny;
d) numer konta bankowego;
e) dane dotyczące rodziny;
f) podstawowe dane dotyczące zdrowia;
g) historia zatrudnienia
h) wykształcenie,
i) zainteresowania.

2. Rodzaje pod-zbiorów zawierających dane osobowe pracowników

Przedsiębiorstwo dokonuje podziału zbioru danych pracowników na pod-zbiory, które utworzone są w oparciu o wyróżniającą cechę kluczową z uwagi na zawartości tego pod-zbioru, lub sposobu pozyskiwania danych do danego pod-zbioru.

Jednie osoby upoważnione do przetwarzania danego pod-zbioru mogą mieć do niego dostęp.

Utworzone zostały następujące pod-zbiory w Przedsiębiorstwie:

a) Akta osobowe,
b) Listy płac,
c) Listy obecności,
d) Rejestr czasu pracy,
e) Rejestr kar dyscyplinarnych.

3. Systemy informatyczne i programy komputerowe, które są lub będą wykorzystywane

Dodatkowe systemy informatyczne i programy komputerowe, które są wykorzystywane, lub będą wykorzystywane przy przetwarzaniu danych osobowych pracowników:

a) Płatnik;

4. Pomieszczenia, w których są przetwarzane dane osobowe pracowników

Dane osobowe pracowników będą mogły być przetwarzanie w ramach sektora Biurowo-administracyjnego.

Dopuszcza się przekazanie do przetwarzania danych osobowych pracowników podmiotu trzeciego – zewnętrznej firmy księgowej lub kadrowej.

5. Czynności przetwarzania danych osobowych pracowników

Przedsiębiorstwo podejmuje następujące czynności przetwarzania danych osobowych pracowników:

a) Rekrutacja – pobranie kwestionariusza CV, listu motywacyjnego, zgody na przetwarzanie danych osobowych.
b) Zatrudnienie – podpisanie umowy, wstępne badania lekarskie, szkolenie BHP, kwestionariusz osoby zatrudnionej.
c) Świadczenie pracy – weryfikacja obecności, rejestracja czasu pracy, wypłata wynagrodzeń, opłacanie należności publiczno-prawnych, nadzór nad obowiązkami pracowniczymi, korzystanie z urlopów.
d) Zakończenie pracy – wydanie świadectwa pracy, wypłata należnych świadczeń.

6. Opis procesu rekrutacyjnego

Rekrutacja odbywa się poprzez umieszczenie ogłoszenia w wybranym serwisie internetowym.

Na podstawie przesłanych dokumentów dokonuje się wstępnej selekcji kandydatów.

Wybrane osoby są zapraszane na rozmowy kwalifikacyjne do siedziby Przedsiębiorstwa.

Rozmowa prowadzona jest przez Zarząd oraz kierownika działu do którego jest nabór.

Zdarza się, że po kilku rozmowach kwalifikacyjnych kandydaci są zapraszani na jeszcze jedną dodatkową rozmowę.

7. Opis czynności związanych z zakończeniem stosunku pracy

Po ustaniu stosunku pracy niezwłocznie wydawane jest świadectwo pracy.
Akta osobowe zostają zarchiwizowane w siedzibie Przedsiębiorstwa.
Konto e-mailowe zostaje dezaktywowane, klucze dostępu odebrane.

8. Dokumenty żądane od pracowników w trakcie zatrudnienia

Rodzaje dokumentów wymaganych od pracowników w trakcie zatrudnienia:

a) Świadectwa pracy,
b) Dyplomy,

c) Certyfikaty
d) Oświadczenia o członkach rodziny podlegających zgłoszeniu do ubezpieczeń
e) Zaświadczenie lekarskie o braku przeciwwskazań do wykonywanej pracy
f) Oświadczenie o niepełnosprawności, przynależności do oddziału NFZ, o podleganiu pod Urząd Skarbowy, o chęci skorzystania z prawa do opieki na dziecko, o zapoznaniu się przepisami BHP, regulacjami wewnętrznymi.

Dokumenty są kompletowane w dziale administracji Przedsiębiorstwa. Zakładane i prowadzone są akta osobowe w formie papierowej. Akta osobowe przechowywane są w szafie zamykanej na klucz.

9. Paski wynagrodzeń

Paski wynagrodzeń są spięte w sposób uniemożliwiający odczyt bez ich zniszczenia.
Rozdawane indywidualnie przez osobę upoważnioną.

DZIAŁ IV: REJESTRY I EWIDENCJE

1. **Rejestr czynności przetwarzania danych osobowych**

Przedsiębiorstwo tworzy i utrzymuje na bieżąco rejestr czynności przetwarzania danych osobowych, który stanowi **załącznik nr 6** do Polityki.

2. **Ewidencja osób upoważnionych do przetwarzania danych osobowych i ich uprawnień**

Przedsiębiorstwo tworzy i utrzymuje na bieżąco ewidencję osób upoważnionych do przetwarzania danych osobowych, która stanowi **załącznik nr 1** do Polityki.

DZIAŁ V: ŚRODKI BEZPIECZEŃSTWA

1. **Środki zabezpieczeń danych osobowych poza systemami informatycznymi**

Rodzaje zabezpieczeń	Sposób realizacji zabezpieczenia - opis
kraty w oknach	
odpowiednie zamki w drzwiach	
magnetyczne karty dostępu	
karty identyfikacyjne	
system kontroli dostępu do pomieszczeń	
fizyczne ograniczenie dostępu do serwerów i infrastruktury sieciowej	
identyfikacja biometryczna	
ochrona fizyczna	
monitoring wizyjny	
systemy alarmowe	
całodobowy monitoring sygnału alarmu	
ograniczenie dostępu do szyfrów rozbrajających alarm	
nadzór nad kluczami do pomieszczeń	
nadzór nad kluczami do szaf, kas	
szafy, kasy pancerne, sejfy	
polityka czystego biurka	
odpowiednie ustawienie monitora	
właściwy obieg dokumentów	
zamknięte skrzynki na dokumenty	
inne: …….	

inne: …….	
inne: …….	

2. Środki zabezpieczeń danych osobowych w systemach informatycznych

Rodzaje zabezpieczeń	Sposób realizacji zabezpieczenia / opis
odpowiednia polityka haseł	
odrębny identyfikator dla każdego użytkownika w systemie informatycznym	
używanie oprogramowania umożliwiającego tworzenie kont użytkowników	
blokada przydzielania tego samego identyfikatora innej osobie	
dostęp do systemu możliwy po wprowadzeniu danych uwierzytelniających	
dostęp do urządzeń po podaniu loginu i hasła	
ograniczenie dostępu użytkownika do określonych zasobów	
monitorowanie dostępu użytkownika do określonych zasobów	
automatyczne wylogowanie z systemu po określonym czasie braku aktywności	
blokowanie możliwości samodzielnej instalacji oprogramowania przez użytkownika	
wybór metod programistycznych	
testowanie jakości aplikacji (przegląd kodu, testy typu czarne skrzynka, testy siłowe)	
pomiar wagi błędów w systemach	
ograniczanie interakcji między użytkownikiem a systemem	
audyt informatyczny	
programy i skanery antywirusowe	
firewall	
strefa zdemilitaryzowana	
rozproszona zapora sieciowa	
proxy	
SSL/VPN/WebVPN/OpenVPN/IPSec	
UTM	
IDS/IPS	
DNS	
DLP	
SNAT	
DNAT	
ISA Server	
DPI	
honeypot	

hping	
skaner portów	
tester pamięci	
snort	
ochrona przed phishingiem	
ochrona przed keyloggerami	
ochrona przed atakami Cross Site Scripting	
ochrona przed Cross Site Request Forgery	
ochrona przed atakami SQL Injection	
autoochrona aplikacji (ochrona aplikacji przed szkodliwym oprogramowaniem)	
kreator analizy bezpieczeństwa	
tworzenie dysku ratunkowego	
antyspyware	
filtr antyspamowy	
filtrowanie treści	
szyfrowanie dysków	
szyfrowanie serwerów	
szyfrowanie wiadomości e-mail, w szczególności zawierających loginy i hasła	
przekazywanie odrębną drogą klucza do zaszyfrowanej wiadomości e-mail (sms, papier, osobiście)	
środki kryptograficzne na potrzeby teletransmisji	
inne środki kryptograficzne	
wykorzystanie macierzy dyskowych do ochrony przed utratą danych	
wykorzystanie VNC, RConsole, TeamViewer (przy ich należytym zabezpieczeniu)	
podtrzymywanie zasilania — UPS/agregaty prądotwórcze/zasilanie z dwóch źródeł	
podtrzymanie bateryjne kontrolera macierzy dyskowej	
regularne aktualizowanie oprogramowania	
domyślne zablokowanie możliwości komunikacji i aktywowanie tych potrzebnych do pracy systemu	
blokowanie zapisu treści na nośniki zewnętrzne, w szczególności blokada portów USB	
zdalne wyłączanie lub blokowanie urządzenia	
zakaz korzystania z niezaufanych punktów dostępu do Internetu (np. w hotelu, kawiarni etc.)	
wykonywanie kopii zapasowych danych	
wykonywanie kopii zapasowych programów	

wykonywanie kopii zapasowych serwerów	
standaryzacja sprzętu	
standaryzacja oprogramowania	
kontrola instalowanego oprogramowania	
pseudonimizacja	
anonimizacja	
inne: …….	
inne: …….	
inne: …….	