.....

pieczęć firmowa

# POLITYKA BEZPIECZEŃSTWA

# DANYCH OSOBOWYCH

**WIELOBRANŻOWE PRZEDSIĘBIORSTWO PRODUKCYJNO USŁUGOWE MOTOS SP. Z O.O.**
**UL. OKULICKIEGO 64, 37 - 450 STALOWA WOLA**

(firma i siedziba przedsiębiorstwa)

Zatwierdzam: STALOWA WOLA, 21 MAJA 2018

miejscowość, data i czytelny podpis osoby upoważnionej


RODO WPPU MOTOS Sp. z o.o.

# ROZDZIAŁ I

# Ogólne zasady polityki bezpieczeństwa danych osobowych

## 1. Podstawowe definicje

1.1. **Administrator danych (ADO) –** podmiot, który decyduje o celach i środkach przetwarzania danych osobowych.

1.2. **Dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej oraz osób fizycznych prowadzących działalność gospodarczą. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne . Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu i działań. Danymi osobowymi będą zatem zarówno takie dane, które pozwalają na określenie tożsamości konkretnej osoby, jak i takie, które nie pozwalają na jej natychmiastową identyfikację, ale są, przy pewnym nakładzie kosztów, czasu i działań, wystarczające do jej ustalenia.

1.3. **Dane wrażliwe** - dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

1.4. **Identyfikator użytkownika** - ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

1.5. **Integralność danych** - właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

1.6. **Nośniki danych** - wszelkie nośniki, na których informacje zapisane są w postaci elektronicznej, w szczególności dyski, dyskietki, dyski CD-ROM, karty magnetyczne lub pamięci przenośne.

1.7. **Odbiorca danych** - każdy, komu udostępnia się dane osobowe, z wyłączeniem: osoby, której dane dotyczą, osoby upoważnionej do przetwarzania danych, przedstawiciela podmiotu przetwarzającego dane osobowe mającego siedzibę lub miejsce zamieszkania w państwie trzecim, podmiotu, któremu powierzono przetwarzanie danych osobowych, organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

1.8. **Personel** - osoby zatrudnione na podstawie stosunku pracy, umów cywilnoprawnych (umowa o dzieło, umowa zlecenia), przedsiębiorcy wykonujący działalność osobiście i jednoosobowo, osoby odbywające praktyki, stażyści, osoby skierowane do pracy w ramach umów z agencjami pracy tymczasowej wykonujące prace związane z przetwarzaniem danych osobowych u administratora danych.

1.9. **Poufność danych** - właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.

1.10. **Przetwarzanie danych osobowych** - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie danych osobowych, w szczególności w systemach informatycznych.

1.11. **Rozliczalność** - właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

1.12. **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programów zastosowanych w celu przetwarzanie danych.

1.13. **Zbiór danych osobowych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

1.14. **Wykaz skrótów:**

1.14.1 **ADO** - Administrator danych

1.14.2 **Ośrodek**
WIELOBRANŻOWE PRZEDSIEBIORSTWO PRODUKCYJNO USŁUGOWE MOTOS SP. Z O.O.
UL. OKULICKIEGO 64
37-450 STALOWA WOLA

1.14.3 **ORGAN** – organ administracji publicznej właściwy do spraw ochrony danych osobowych,

1.14.4 **Ustawa** - Ustawa o ochronie danych osobowych.

## 2. Wprowadzenie

2.1. OŚRODEK opracowuje i zatwierdza politykę bezpieczeństwa danych osobowych jako wyraz woli wdrożenia przepisów prawnych dotyczących ochrony danych osobowych.

2.2. Celem polityki bezpieczeństwa danych osobowych jest wskazanie działań jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie zabezpieczać dane osobowe, a zatem organizacyjne, fizyczne i logiczne zabezpieczenie posiadanych danych osobowych oraz edukowanie użytkowników systemu ochrony danych osobowych. Polityka bezpieczeństwa danych osobowych określa zadania związane z zachowaniem poufności, integralności oraz rozliczalności danych osobowych.

2.3. Zasady określone przez dokument polityka bezpieczeństwa danych osobowych mają zastosowanie do wszystkich:

2.3.1 danych osobowych przetwarzanych przez OŚRODEK, zarówno w przypadku, gdy jest administratorem danych, jak i w sytuacji, gdy przetwarza dane powierzone na podstawie umów zawartych w trybie art. 31 Ustawy o ochronie danych osobowych,

2.3.2 nośników informacji, np. papierowych, magnetycznych, optycznych itp., na których są lub będą znajdować się dane osobowe,

2.3.3 lokalizacji - budynków i pomieszczeń OŚRODEK, w których są lub będą przetwarzane dane osobowe,

2.3.4 osób stanowiących personel,

2.3.5 innych osób mających dostęp do danych osobowych.

2.4. Polityka bezpieczeństwa nie obejmuje obszaru i systemu informatycznego oraz środków technicznych i organizacyjnych zastosowanych przez podmioty, którym zostały powierzone dane osobowe w drodze umowy zawartej na piśmie.

2.5. Osoby stanowiące personel OŚRODEK oraz wszystkie inne mające dostęp do tych danych zobowiązane są do przestrzegania postanowień polityki bezpieczeństwa danych osobowych.

2.6. Polityka bezpieczeństwa danych osobowych powinna być poddawana bieżącej aktualizacji, ale nie rzadziej niż raz do roku.

2.7. Jeżeli przepisy innych ustaw przewidują dalej idącą ochronę danych osobowych niż ustawa o ochronie danych osobowych, stosuje się przepisy tych ustaw.

# 3. Wykaz zbiorów oraz obowiązki w zakresie ochrony danych osobowych

3.1. **OŚRODEK jest ADO dla następujących zbiorów:**

3.1.1 "Kursanci"

3.1.2 "Marketing".

3.1.3 "Kontakty służbowe"

3.1.4 "Umowy cywilnoprawne"

3.2. **Obowiązki ADO obejmują**:

3.2.1 Zapewnienie środków technicznych i organizacyjnych do ochrony przetwarzanych danych osobowych, odpowiednio do zagrożeń oraz kategorii danych objętych ochroną, w szczególności zabezpieczeniem danych przed:

- udostępnieniem osobom nieupoważnionym,
- zabraniem przez osobę nieuprawnioną,
- zmianą, utratą, uszkodzeniem lub zniszczeniem.

3.2.2 Zapewnienie legalności przetwarzania danych osobowych, a w szczególności zadbanie, by:

- została pozyskana zgoda osoby, której dane dotyczą lub została spełniona inna przesłanka dopuszczająca przetwarzanie danych osobowych,
- został spełniony obowiązek informacyjny wobec osoby, której dane dotyczą,
- dane były przetwarzane zgodnie z obowiązującymi przepisami prawa, dobrymi praktykami oraz normami społecznymi,
- dane zbierane były w oznaczonym zgodnym z prawem celem,
- dane były merytorycznie poprawne oraz zakres danych był adekwatny do celu zbierania,
- dane były przetwarzane z ograniczeniem czasowym.

3.2.3 Zatwierdzenie dokumentacji opisującej sposób przetwarzania danych osobowych, w szczególności:

- Polityki bezpieczeństwa danych osobowych,
- Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

3.2.4 Dopuszczanie do przetwarzania danych wyłącznie osoby przeszkolonej i posiadającej upoważnienie, oraz wydawanie i zarządzanie upoważnieniami.

3.2.5 Nadzorowanie i dbanie o zgodne z prawem przekazywanie danych osobowych (udostępnianie i powierzanie).

3.2.6 Respektowanie prawa osób, których dane dotyczą, a w szczególności prawa do uzyskania informacji o:

- administratorze danych,
- celu, zakresie i sposobie przetwarzania danych,
- terminu od kiedy i jakie dane są przetwarzane,
- źródle, z którego dane pochodzą,
- sposobie udostępniania danych oraz ich odbiorcach.

3.2.7 Respektowanie praw osób, których dane dotyczą w zakresie:

- żądania uzupełnienia, uaktualnienia, sprostowania danych,
- wniesienia umotywowanego wniosku do zaprzestania przetwarzania danych,
- wycofania zgody na przetwarzanie danych osobowych.

3.2.8 Prowadzenie rejestru czynności przetwarzania danych osobowych w zakresie wymaganym przez obowiązujące przepisy.

3.2.9 Zapewnienie przeprowadzenia regularnych wewnętrznych audytów przestrzegania przepisów dotyczących ochrony danych osobowych.

3.3. **OŚRODEK przetwarza dane osobowe na podstawie umowy powierzenia jako procesor.**

3.3.1 Obowiązki w zakresie zbiorów powierzonych:

3.3.2 Zapewnienie środków technicznych i organizacyjnych do ochrony przetwarzanych danych osobowych, odpowiednio do zagrożeń oraz kategorii danych objętych ochroną, w szczególności zabezpieczeniem danych przed:

- udostępnieniem osobom nieupoważnionym,
- zabraniem przez osobę nieuprawnioną,
- zmianą, utratą, uszkodzeniem lub zniszczeniem.

3.3.3 Prowadzenie dokumentacji opisującej sposób przetwarzania danych osobowych, w szczególności:

- Polityki bezpieczeństwa danych osobowych,
- Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

3.3.4 Dopuszczanie do przetwarzania danych wyłącznie osoby przeszkolonej i posiadającej upoważnienie, oraz wydawanie i zarządzanie upoważnieniami.

3.3.5 Nadzorowanie i dbanie o zgodne z prawem przekazywanie danych osobowych (udostępnianie i powierzanie).

3.3.6 Nadzorowanie zadań w zakresie:

- przeglądu, konserwacji oraz uaktualnienia systemów służących do przetwarzania danych,
- kontroli systemu komunikacji w sieci komputerowej,
- uwierzytelniania personelu, w szczególności poprzez nadawanie zmian lub pozbawienie uprawnień dostępu do systemu użytkowników,
- wykonywania polityki ochrony antywirusowej,
- wykonywania kopii bezpieczeństwa.

3.3.7 Przeprowadzanie regularnych wewnętrznych audytów przestrzegania przepisów dotyczących ochrony danych osobowych.

## 4. Dane wrażliwe

4.1. Zabrania się przetwarzania "danych wrażliwych" ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

4.2. Przetwarzanie "danych wrażliwych" jest jednak dopuszczalne, pod następującymi warunkami:

4.2.1 osoba , której dane dotyczą, wyrazi na to zgodę na piśmie, chyba że chodzi o usunięcie dotyczących jej danych,

4.2.2 przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony,

4.2.3 przetwarzanie takich danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora,

4.2.4 przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem,

4.2.5 przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób stanowiących personel, a zakres przetwarzanych danych jest określony w ustawie,

4.2.6 przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą,

4.2.7 przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.

## 5. Powierzanie przetwarzania danych osobowych

5.1. Administrator danych może powierzyć przetwarzanie danych osobowych innemu podmiotowi w drodze umowy zawartej na piśmie.

5.2. Przekazanie zbiorów podmiotowi zewnętrznemu w celu ich przetwarzania nie powoduje zmiany właściwego administratora danych.

5.3. Podmiot zewnętrzny, któremu powierzono przetwarzanie danych obowiązany jest wykorzystywać powierzone mu dane wyłącznie w celach i w zakresie, które zostały wskazane w zawartej z nim umowie.

5.4. Podmiot zewnętrzny, któremu powierzono przetwarzanie danych obowiązany jest między innymi do:

5.4.1 stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,

5.4.2 opracowania dokumentacji dotyczącej przetwarzania danych osobowych,

5.4.3 zapewnienia, aby do przetwarzania danych mogły być dopuszczone wyłącznie osoby posiadające upoważnienie,

5.4.4 zapewnienia kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane,

5.4.5 prowadzenia ewidencji osób upoważnionych do ich przetwarzania,

5.4.6 obowiązania osób, które zostały upoważnione do przetwarzania danych do zachowania w tajemnicy tych danych osobowych oraz sposobów ich zabezpieczania.

## 6. Zasady udostępniania danych osobowych

6.1. Udostępnianie danych jest jedną z form ich przetwarzania.

6.2. Udostępnianie danych osobowych odbiorcom danych może nastąpić, podobnie jak przetwarzanie danych, w przypadku spełnienia jednej z przesłanek określonych w art. 23 ust. 1 pkt 1-5 Ustawy o ochronie danych osobowych:

6.2.1 osoba, której dane dotyczą, wyrazi na to zgodę,

6.2.2 jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa,

6.2.3 jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,

6.2.4 jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,

6.2.5 jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

6.3. Zgodnie z art. 38 Ustawy o ochronie danych osobowych administrator danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy oraz komu zostały przekazane.

## 7. Przekazywanie danych osobowych do państwa trzeciego

7.1. Administrator danych może przekazać dane osobowe do państwa trzeciego, jeżeli:

7.1.1 państwo docelowe daje gwarancje ochrony danych osobowych na swoim terytorium przynajmniej takie, jakie obowiązują na terytorium Rzeczypospolitej Polskiej,

7.1.2 odpowiedni poziom ochrony danych osobowych, o którym mowa powyżej, jest oceniany z uwzględnieniem wszystkich okoliczności dotyczących operacji przekazania danych, w szczególności biorąc pod uwagę charakter danych, cel i czas trwania proponowanych operacji przetwarzania danych, kraj pochodzenia i kraj ostatecznego przeznaczenia danych oraz przepisy prawa obowiązujące w danym państwie trzecim oraz stosowane w tym państwie środki bezpieczeństwa i zasady zawodowe,

7.1.3 przesłanie danych osobowych wynika z obowiązku nałożonego na administratora danych przepisami prawa lub postanowieniami ratyfikowanej umowy międzynarodowej,

7.1.4 osoba, której dane dotyczą udzieliła na to zgody na piśmie,

7.1.5 przekazanie jest niezbędne do wykonania umowy pomiędzy administratorem danych a osobą, której dane dotyczą, lub jest podejmowane na jej życzenie,

7.1.6 przekazanie jest niezbędne do wykonania umowy zawartej w interesie osoby, której dane dotyczą, pomiędzy administratorem danych a innym podmiotem,

7.1.7 przekazanie jest niezbędne ze względu na dobro publiczne lub do wykazania zasadności roszczeń prawnych,

7.1.8 przekazanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą,

7.1.9 dane są ogólnie dostępne.

# ROZDZIAŁ II

# Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych osobowych

## 8. Środki ochrony fizycznej danych osobowych

8.1. Pomieszczenia, w którym przetwarzane są zbiory danych osobowych zabezpieczone są przed próbami uzyskania nieuprawnionego dostępu do nich poprzez urządzenia alarmowe, dozór lub inne środki.
8.2. W pomieszczeniach, w których przetwarzane są zbiory danych osobowych znajdują się gaśnice.
8.3. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.
8.4. Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym standardowymi drzwiami biurowymi.
8.5. Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej niemetalowej szafie.

## 9. Środki sprzętowe, infrastruktury informatycznej i telekomunikacyjnej oraz narzędzia programowe i baz danych zastosowane w celu ochrony danych osobowych

9.1. Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.
9.2. Użyto system Firewall do ochrony dostępu do sieci komputerowej.
9.3. Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
9.4. Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.
9.5. Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji
9.6. Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych.
9.7. Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych.
9.8. Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych.
9.9. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

9.10. Zastosowano urządzenia UPS chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.
9.11. Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.
9.12. Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
9.13. Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.

## 10. Środki organizacyjne zastosowane w celu ochrony danych osobowych

10.1. Osoby przetwarzające dane osobowe zostały:
  10.1.1 zaznajomione z przepisami dotyczącymi ochrony danych osobowych,
  10.1.2 przeszkolone w zakresie zabezpieczeń systemu informatycznego,
  10.1.3 upoważnione do przetwarzania danych osobowych
  10.1.4 zobowiązane do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczania.
10.2. OŚRODEK prowadzi rejestr czynności przetwarzania danych osobowych.
10.3. OŚRODEK prowadzi rejestr osób upoważnionych.
10.4. Wdrożona została dokumentacja dotycząca ochrony danych osobowych: polityka bezpieczeństwa danych osobowych oraz instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
10.5. OŚRODEK przeprowadza regularne przeglądy polityki bezpieczeństwa danych osobowych oraz instrukcji zarządzania systemem informatycznym.
10.6. Przekazywanie danych osobowych do podmiotów trzecich (udostępnianie i powierzanie) jest nadzorowane oraz odbywa się na zasadach zgodnych z przepisami powszechnie obowiązującego prawa.