1. **OGÓLNE WYTYCZNE ORAZ ZASADY POSTĘPOWANIA Z DANYMI OSOBOWYMI PRZEZ WYKONAWCĘ I PODWYKONAWCĘ**
2. **Postanowienia ogólne**

# Definicje dotyczące przetwarzania danych osobowych:

W niniejszej załączniku poniższe terminy mają następujące znaczenie, a terminy pokrewne należy interpretować zgodnie z nimi:

1. *„Administrator” – Zamawiający* Podkarpacki Zarząd Dróg Wojewódzkich w Rzeszowie
2. „Podmiot Przetwarzający”, - Wykonawca
3. *Podwykonawcy Przetwarzania”* - Podwykonawca

- Podwykonawców Przetwarzania wskazanych w Umowie Głównej ; oraz

- dodatkowych Podwykonawców Przetwarzania, o których Wykonawca poinformował Administratoraw trakcie realizacji Umowy Głównej

1. *„Podwykonawca Przetwarzania”* oznacza każdy Podmiot Przetwarzający Dane (w tym stronę trzecią) wyznaczony przez Podmiot Przetwarzający do przetwarzania Danych Osobowych Administratora w jego imieniu.
2. *„Przetwarzać/Przetwarzanie/Przetwarzane”, „Administrator Danych”, „Podmiot Przetwarzający Dane”, „Osoba, której Dane Dotyczą”, „Dane Osobowe”, „Szczególne Kategorie Danych Osobowych”* i inne terminy nieuwzględnione w niniejszej Umowie lub Umowie Głównej mają takie samo znaczenie jak określono w Rozporządzeniu o Ochronie Danych Osobowych 2016/679 Parlamentu Europejskiego i Rady („RODO”).
3. *„Przepisy o Ochronie Danych”* oznaczają Rozporządzenie o Ochronie Danych Osobowych 2016/679 Parlamentu Europejskiego i Rady („RODO”) oraz wszelkie inne lokalne przepisy o ochronie danych.
4. *„Usunięcie”* oznacza usunięcie lub zniszczenie Danych Osobowych w sposób uniemożliwiający ich odzyskanie lub odtworzenie.
5. *„Państwo Trzecie”* oznacza państwo leżące poza terytorium UE/EOG, z wyjątkiem państwa, wobec którego Komisja Europejska wydała ważną decyzję stwierdzającą odpowiedni stopień ochrony Danych Osobowych.
6. *„Dane Osobowe Administratora”* oznaczają Dane Osobowe przetwarzane przez Podmiot Przetwarzający w imieniu Administratora zgodnie z Umową Główną lub w związku z nią.
7. *„Naruszenie Ochrony Danych Osobowych”* oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do Danych Osobowych Administratora przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
8. *„Usługi*” oznaczają usługi, które mają być świadczone przez Podmiot Przetwarzający na rzecz Administratora zgodnie z Umową Główną.
9. *„Produkty”* oznaczają produkty, które mają zostać dostarczone Administratorowi przez Podmiot Przewarzający zgodnie z Umową Główną.
10. *„Standardowe Klauzule Umowne”* oznaczają standardowe klauzule umowne dotyczące przekazywania danych osobowych Podmiotom Przetwarzającym prowadzącym działalność w państwach trzecich, zatwierdzone Decyzją 2010/87/UE Komisji Europejskiej, lub jakikolwiek zbiór klauzul zatwierdzony przez Komisję Europejską, który je zmienia lub zastępuje.
11. **Skróty**

"EOG" oznacza Europejski Obszar Gospodarczy.

1. **Powierzenie dostawcy przetwarzania danych osobowych**

Terminy niezdefiniowane inaczej w niniejszym dokumencie mają znaczenie przypisane im w Umowie Głównej. Z wyjątkiem zmian wprowadzonych poniżej warunki Umowy Głównej pozostają w pełni obowiązujące i skuteczne.

# Warunki przetwarzania danych

4.1. Dostarczając Administratorowi Usługi i/lub Produkty na mocy Umowy Głównej, Podmiot Przetwarzający może przetwarzać dane osobowe Administratora w jego imieniu zgodnie z warunkami niniejszego Dodatku. Podmiot Przetwarzający wyraża zgodę na przestrzeganie następujących postanowień dotyczących danych osobowych Administratora.

4.2. W zakresie wymaganym przez obowiązujące Przepisy o Ochronie Danych Podmiot Przetwarzający uzyska i utrzyma wszelkie licencje, upoważnienia i pozwolenia potrzebne do przetwarzania danych osobowych.

Podmiot Przetwarzający jest zobowiązany stosować wszelkie techniczne i organizacyjne środki pozwalające na spełnienie wymogów określonych w Dodatku.

# Przetwarzanie danych osobowych administratora

* 1. Wykonawca przed przystąpieniem do wykonania umowy jest zobowiązany przeprowadzić szkolenia wszystkich osób uczestniczących w realizacji zamówienia z zakresu stosowania przepisów o ochronie danych osobowych. Podmiot Przetwarzający będzie przetwarzał Dane Osobowe Administratora jedynie do celów Umowy Głównej. Podmiot Przetwarzający nie będzie przetwarzał, przekazywał, modyfikował, zmieniał lub korygował Danych Osobowych Administratora, a także ujawniał lub zezwalał na ujawnienie danych osobowych Administratora stronom trzecim bez udokumentowanych wytycznych Administratora, chyba że przetwarzanie jest wymagane przez przepisy prawa UE lub państwa członkowskiego, którym podlega Podmiot Przetwarzający. Przed rozpoczęciem przetwarzania Danych Osobowych Podmiot Przetwarzający zawiadomi Administratora, w zakresie dozwolonym przez rzeczone prawo, o takim wymogu prawnym i dostosuje się do wytycznych Administratora w celu ograniczenia, w największym możliwym zakresie, takiego ujawnienia.
  2. W celach określonych w powyższym ustępie Administrator niniejszym zleca Podmiotowi Przetwarzającemu przekazanie Danych Osobowych Administratora odbiorcom w Państwach Trzecich pod warunkiem że Podmiot Przetwarzający przestrzega postanowień artykułu o Podwykonawstwie Przetwarzania art. 44-49 RODO.

# Rzetelność i zachowanie poufności

* 1. Podmiot Przetwarzający podejmie rozsądne działania w celu zapewnienia, by wszyscy pracownicy, przedstawiciele lub wykonawcy, którzy mogą mieć dostęp do danych osobowych Administratora, postępowali rzetelnie, gwarantując, że w każdym przypadku dostęp do Danych Osobowych Administratora zostanie przyznany tylko i wyłącznie tym osobom, dla których jest niezbędny.
  2. Podmiot Przetwarzający jest zobowiązany zapewnić, by wszystkie osoby, których obowiązkiem jest przetwarzanie danych osobowych administratora:
  3. Zostały poinformowane o poufnym charakterze Danych Osobowych Administratora i miały świadomość zobowiązań Podmiotu Przetwarzającego wynikających z niniejszego Dodatku oraz Umowy Głównej w związku z Danymi Osobowymi Administratora;
     1. Odbyły odpowiednie szkolenie/uzyskały odpowiednie certyfikaty dotyczące Przepisów o Ochronie Danych lub odbyły inne szkolenia/uzyskały inne certyfikaty wymagane przez Administratora;
     2. Podlegały zobowiązaniu do zachowania poufności lub tajemnicy zawodowej lub ustawowemu obowiązkowi zachowania poufności; oraz
     3. Podlegały uwierzytelnieniu użytkownika i procedurze logowania w celu uzyskania dostępu do Danych Osobowych Administratora zgodnie z niniejszą Umową, Umową Główną i obowiązującymi Przepisami o Ochronie Danych.

# Bezpieczeństwo danych osobowych

* 1. Uwzględniając stan wiedzy technicznej, koszty wdrożenia, charakter, zakres, kontekst i cele Przetwarzania, a także ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, Podmiot Przetwarzający musi zastosować odpowiednie środki techniczne lub organizacyjne aby zapewnić stopień bezpieczeństwa Danych Osobowych Administratora odpowiadający temu ryzyku, w tym między innymi:

### Pseudonimizację i szyfrowanie danych osobowych;

### Zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;

### Zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego; oraz

### Regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo Przetwarzania.

### Oceniając, czy stopień bezpieczeństwa jest odpowiedni, Podmiot Przetwarzający uwzględnia w szczególności ryzyko wiążące się z przetwarzaniem, a zwłaszcza wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych

# Podwykonawstwo przetwarzania

## Począwszy od Dnia Wejścia w Życie Dodatku Administrator niniejszym upoważnia Podmiot Przetwarzający do skorzystania z usług Podwykonawców Przetwarzania.

## 8.2. W odniesieniu do każdego Podwykonawcy Przetwarzania Podmiot Przetwarzający przed przystąpieniem do wykonania umowy jest zobowiązany poinformować podwykonawcę o obowiązku przeprowadzenia szkolenia wszystkich osób uczestniczących w realizacji zamówienia z zakresu stosowania przepisów o ochronie danych osobowych, ponadto na, pisemne żądanie Administratora jest zobowiązany:

### Przedstawić Administratorowi kompletne informacje na temat Przetwarzania, którego ma się podjąć każdy Podwykonawca Przetwarzania.

### Przeprowadzić odpowiednią analizę każdego Podwykonawcy Przetwarzania pod kątem zgodności ze standardami należytej staranności (due diligence), aby potwierdzić, że może on zapewnić właściwy stopień ochrony Danych Osobowych Administratora, w tym między innymi wystarczające gwarancje wdrożenia odpowiednich technicznych i organizacyjnych środków w celu spełnienia wymogów RODO, niniejszej Umowy, Umowy Głównej i obowiązujących Przepisów o Ochronie Danych w zakresie Przetwarzania.

### W umowie pomiędzy Podmiotem Przetwarzającym a każdym Podwykonawcą Przetwarzania uwzględnić te same warunki, które zostały określone w niniejszym Dodatku. Podmiot Przetwarzający dostarczy do wglądu Administratorowi kopię umów zawartych z Podwykonawcami Przetwarzania na jego żądanie.

### W zakresie, w jakim umowa dotyczy przekazywania Danych Osobowych Administratora poza terytorium EOG, włączyć do umowy między Podmiotem Przetwarzającym a każdym Podwykonawcą Przetwarzania Standardowe Klauzule Umowne lub inny mechanizm wskazany przez Administratora w celu zapewnienia odpowiedniej ochrony przekazywanych Danych Osobowych Administratora.

### Ponosić całkowitą odpowiedzialność wobec Administratora za każdy przypadek niewypełnienia zobowiązań Podwykonawcy Przetwarzania dotyczących Przetwarzania Danych Osobowych Administratora.

## Począwszy od Dnia Wejścia w Życie Dodatku Administrator niniejszym upoważnia Podmiot Przetwarzający do skorzystania z usług Podwykonawców Przetwarzania

**- ogólna zgoda Administratora art. 28 ust. 2 RODO, podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.**

# 9. Prawa osób, których dane dotyczą

# 9.1. Uwzględniając charakter Przetwarzania, Podmiot Przetwarzający jest zobowiązany w miarę możliwości pomóc Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania Osoby, której Dane Dotyczą, w zakresie wykonywania jej praw określonych w RODO.

## 9.2. Podmiot Przetwarzający niezwłocznie powiadomi Administratora o otrzymaniu żądania od Osoby, której Dane Dotyczą, od Organu Nadzorczego i/lub innego właściwego organu na mocy obowiązujących Przepisów o Ochronie Danych dotyczącego Danych Osobowych Administratora.

## 9.3. Na żądanie Administratora Podmiot Przetwarzający będzie z nim współpracował, aby umożliwić Administratorowi zastosowanie się do wymogów realizacji praw Osoby, której Dane Dotyczą, na mocy Przepisów o Ochronie Danych w odniesieniu do Danych Osobowych Administratora, a także zastosowanie się do jakiejkolwiek oceny, zapytania, zawiadomienia lub postępowania wyjaśniającego wynikających z Przepisów o Ochronie Danych dotyczących Danych Osobowych Administratora lub niniejszej Umowy, a współpraca ta będzie obejmować:

### 9.4. Dostarczenie wszystkich danych wymaganych przez Administratora w rozsądnym terminie określonym w każdym przypadku przez Administratora, w tym kompletnych informacji dotyczących skargi, korespondencji lub żądania oraz kopii tych dokumentów, a także wszelkich Danych Osobowych Administratora, które Podmiot Przetwarzający przechowuje na temat Osoby, której Dane Dotyczą.

### 9.5. Jeśli ma to zastosowanie, udzielenie pomocy w zakresie zasadnie wymaganym przez Administratora, aby umożliwić mu spełnienie odpowiedniego żądania w terminie określonym Przepisami o Ochronie Danych.

### 9.6. Zastosowanie dodatkowych technicznych i organizacyjnych środków na zasadne żądanie Administratora, aby umożliwić mu skuteczną reakcję na skargi, zawiadomienia lub żądania.

# 10. Naruszenie ochrony danych osobowych

## Podmiot Przetwarzający niezwłocznie zawiadomi Administratora, a w każdym przypadku w ciągu dwudziestu czterech godzin (24), o stwierdzeniu lub uzasadnionym podejrzeniu Naruszenia Ochrony Danych Osobowych. Podmiot Przetwarzający dostarczy Administratorowi informacje wystarczające do tego, by Administrator mógł wywiązać się z obowiązku zgłoszenia Naruszenia Ochrony Danych Osobowych wynikającego z Przepisów o Ochronie Danych. Takie zgłoszenie musi co najmniej:

### Opisywać charakter Naruszenia Ochrony Danych Osobowych, wskazywać kategorie i liczbę Osób, których Dane Dotyczą, oraz kategorie i liczbę wpisów Danych Osobowych, których dotyczy naruszenie;

### Zawierać imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych Podmiotu Przetwarzającego, Pełnomocnika ds. Prywatności lub wskazanie innego punktu kontaktowego, od którego można uzyskać więcej informacji;

### Opisywać przewidywane zagrożenie oraz możliwe konsekwencje Naruszenia Danych Osobowych; oraz

### Opisywać środki zastosowane lub proponowane w celu zaradzenia Naruszeniu Ochrony Danych Osobowych.

## 10.2. Podmiot Przetwarzający zobowiązuje się współpracować z Administratorem i podjąć zasadne działania handlowe zalecone przez Administratora, aby udzielić wsparcia w postępowaniu wyjaśniającym, wdrażaniu środków łagodzących i zaradczych związanych z każdym Naruszeniem Ochrony Danych Osobowych.

## 10.3. W przypadku Naruszenia Ochrony Danych Osobowych przed poinformowaniem jakiejkolwiek strony trzeciej Podmiot Przetwarzający jest zobowiązany najpierw uzyskać pisemną zgodę Administratora, chyba że takie zawiadomienie jest wymagane przepisami prawa UE lub państwa członkowskiego obowiązującymi Podmiot Przetwarzający, w którym to przypadku Podmiot Przetwarzający, w zakresie dozwolonym przez takie prawo, zawiadomi Administratora o tym wymogu prawnym, dostarczy kopię proponowanego zawiadomienia i uwzględni wszelkie uwagi Administratora przed zgłoszeniem Naruszenia Ochrony Danych Osobowych.

# 11. Ocena skutków w zakresie ochrony danych i uprzednia konsultacja

Podmiot Przetwarzający jest zobowiązany udzielić zasadnej pomocy Administratorowi przy ocenie skutków w zakresie ochrony danych wymaganej na mocy Artykułu 35 RODO oraz przy uprzedniej konsultacji z organem nadzorczym Administratora przewidzianej Artykułem 36 RODO, w każdym przypadku wyłącznie w związku z Przetwarzaniem Danych Osobowych Administratora przez Podmiot Przetwarzający w imieniu Administratora i z uwzględnieniem charakteru przetwarzania oraz informacji dostępnych Podmiotowi Przetwarzającemu.

# 12. Usunięcie lub zwrot danych osobowych administratora

## 12.1 Podmiot Przetwarzający niezwłocznie i w każdym przypadku w ciągu 90 (dziewięćdziesięciu) dni kalendarzowych od chwili: (i) zaprzestania Przetwarzania Danych Osobowych Administratora przez Podmiot Przetwarzający; lub (ii) zakończenia Umowy Głównej, w zależności od tego, które z tych zdarzeń nastąpi wcześniej, zgodnie z decyzją Administratora (decyzja musi zostać dostarczona Podmiotowi Przetwarzającemu na piśmie):

### Zwróci Administratorowi kompletną kopię wszystkich Danych Osobowych Administratora za pomocą bezpiecznego transferu plików w formacie wskazanym przez Administratora i trwale usunie wszystkie inne kopie Danych Osobowych Administratora Przetwarzanych przez Podmiot Przetwarzający lub Podwykonawcę Przetwarzania; lub

### Trwale skasuje wszystkie kopie Danych Osobowych Administratora Przetwarzanych przez Podmiot Przetwarzający lub Podwykonawcę Przetwarzania i w każdym przypadku przedstawi Administratorowi pisemne zaświadczenie stwierdzające całkowite wywiązanie się ze zobowiązań określonych w artykule Usunięcie lub Zwrot Danych Osobowych Administratora.

### Podmiot Przetwarzający może zachować Dane Osobowe Administratora w zakresie wymaganym przez prawo Unii Europejskiej lub państwa członkowskiego i wyłącznie w takim zakresie oraz przez taki okres, jaki przewiduje prawo Unii Europejskiej lub państwa członkowskiego, pod warunkiem że Podmiot Przetwarzający zapewni poufność wszystkich Danych Osobowych Administratora i zagwarantuje, że będą one przetwarzane tylko w stopniu niezbędnym do realizacji celów przewidzianych prawem Unii Europejskiej lub państwa członkowskiego, które wymaga ich przechowywania, i nie do żadnych innych celów.

# Prawa dotyczące audytu

Podmiot Przetwarzający udostępni Administratorowi na jego żądanie wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym Dodatku oraz umożliwi Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji wszelkich obiektów, w których odbywa się Przetwarzanie Danych Osobowych Administratora, i przyczyni się do nich. Podmiot Przetwarzający zezwoli Administratorowi lub audytorowi upoważnionemu przez Administratora na przejrzenie, zbadanie i skopiowanie wszelkich wpisów, procedur i systemów, aby Administrator mógł się upewnić, że postanowienia niniejszego Dodatku są przestrzegane. Podmiot Przetwarzający jest zobowiązany do pełnej współpracy z Administratorem w przypadku takiego audytu i na żądanie Administratora dostarczy mu dowód stwierdzający wywiązanie się z obowiązków wynikających z niniejszego Dodatku. Podmiot Przetwarzający niezwłocznie powiadomi Administratora, jeśli jego zdaniem zalecenie wydane na podstawie niniejszego Artykułu (Prawa dotyczące audytu) jest sprzeczne z postanowieniami RODO lub innymi postanowieniami UE lub państwa członkowskiego w zakresie ochrony danych.

# Międzynarodowe przekazywanie danych osobowych administratora

## Podmiot Przetwarzający nie może przetwarzać Danych Osobowych Administratora lub zezwolić Podwykonawcy Przetwarzania na przetwarzanie Danych Osobowych Administratora w Państwie Trzecim w odniesieniu do innych odbiorców w Państwach chyba że uzyska wcześniejszą pisemną zgodę Administratora za pomocą zmiany wprowadzonej do niniejszego Dodatku.

## Na żądanie Administratora Podmiot Przetwarzający niezwłocznie zawrze (lub zapewni, by odnośny Podwykonawca Przetwarzania Podmiotu Przetwarzającego zawarł) umowę z Administratorem uwzględniającą Standardowe Klauzule Umowne i/lub jej zmienioną wersję zgodnie z wymogami Przepisów o Ochronie Danych Osobowych dotyczącą przetwarzania Danych Osobowych Administratora w Państwie Trzecim, a jej postanowienia będą nadrzędne wobec postanowień niniejszego Dodatku.

# Kodeksy postępowania i certyfikacja

Na żądanie Administratora Podmiot Przetwarzający będzie stosował zasady Kodeksu Postępowania zatwierdzonego zgodnie z Artykułem 40 RODO i uzyska certyfikację zatwierdzoną na mocy Artykułu 42 RODO w zakresie, w jakim odnoszą się one do przetwarzania Danych Osobowych Administratora.

# Warunki ogólne

## Postanowienia niniejszego dodatku wygasają z chwilą zakończenia umowy.

## Wszelkie zobowiązania Podmiotu Przetwarzającego wynikające z niniejszego Dodatku związane z Przetwarzaniem Danych Osobowych pozostaną w mocy po rozwiązaniu lub wygaśnięciu niniejszego Dodatku.

## Niniejszy Dodatek, z wyłączeniem Standardowych Klauzul Umownych, podlega prawu właściwemu określnemu w Umowie Głównej, pod warunkiem że to prawo właściwe jest prawem państwa członkowskiego Unii Europejskiej.

## W odniesieniu do przedmiotu niniejszego Dodatku w przypadku rozbieżności między postanowieniami Dodatku a postanowieniami innych umów zawartych między stronami, w tym między innymi Umowy Głównej, postanowienia niniejszego Dodatku będą miały moc rozstrzygającą w zakresie zobowiązań stron dotyczących ochrony Danych Osobowych Osoby, której Dane Dotyczą, z państwa członkowskiego Unii Europejskiej.

## Jeśli którekolwiek z postanowień niniejszego Dodatku okaże się nieważne lub niewykonalne, pozostałe postanowienia Dodatku pozostaną ważne i obowiązujące. Nieważne lub niewykonalne postanowienie zostanie

## zmienione w stopniu umożliwiającym uzyskanie jego ważności lub wykonalności przy jednoczesnym zachowaniu, w miarę możliwości, intencji stron, lub

## zinterpretowane w taki sposób, jakby jego nieważna lub niewykonalna część nie została w nim umieszczona.

**II. ŚRODKI TECHNICZNE I ORGANIZACYJNE**

1. **Organizacyjne środki bezpieczeństwa**
   1. **Zarządzanie bezpieczeństwem**
2. Polityka i procedury bezpieczeństwa: Podmiot Przetwarzający jest zobowiązany do udokumentowania polityki bezpieczeństwa w zakresie przetwarzania danych osobowych.
3. Funkcje i obowiązki:
   1. Funkcje i obowiązki związane z przetwarzaniem danych osobowych zostały wyraźnie określone i rozdzielone zgodnie z polityką bezpieczeństwa.
   2. Podczas wewnętrznej reorganizacji lub rozwiązania i zmiany stosunku pracy wyraźnie określa się zasady unieważnienia praw i obowiązków oraz odnośnej procedury ich przekazania.
4. Polityka w zakresie kontroli dostępu: Każdej osobie pełniącej określone funkcje związane z przetwarzaniem danych osobowych przyznawane są konkretne prawa dostępu zgodnie z zasadą wiedzy koniecznej.
5. Zarządzanie zasobami/aktywami: Podmiot Przetwarzający prowadzi rejestr zasobów IT wykorzystywanych do przetwarzania danych osobowych (sprzęt komputerowy, programy komputerowe i sieć). Za prowadzenie i aktualizację rejestru jest odpowiedzialna wyznaczona do tej funkcji osoba (np. specjalista ds. IT).
6. Zarządzanie zmianami: Podmiot Przetwarzający zapewnia, by wszystkie zmiany w systemie IT zostały zarejestrowane i nadzorowane przez określoną osobę (np. specjalistę ds. IT lub bezpieczeństwa). Proces jest regularnie monitorowany.
   1. **Reagowanie na incydenty i ciągłość działania**
7. Obsługa incydentów / Naruszenia ochrony danych osobowych:
   1. W celu zapewnienia skutecznej i należytej reakcji na incydenty dotyczące danych osobowych opracowano plan reagowania na incydenty ze szczegółowymi procedurami.
   2. Podmiot Przetwarzający bezzwłocznie zgłosi Administratorowi wszelkie incydenty naruszenia bezpieczeństwa, które doprowadziły do utraty, niewłaściwego użycia lub nieuprawnionego pozyskania danych osobowych.
8. Ciągłość działania: Podmiot Przetwarzający wprowadza główne procedury i mechanizmy kontrolne obowiązujące w celu zapewnienia wymaganego poziomu ciągłości działania i dostępności systemu IT przetwarzającego dane osobowe (w przypadku wystąpienia incydentu/naruszenia danych osobowych).
   1. **Zasoby ludzkie**
9. Zachowanie poufności przez personel: Podmiot Przetwarzający zapewnia, by wszyscy pracownicy rozumieli swoje obowiązki związane z przetwarzaniem danych osobowych. Informacje o funkcjach i obowiązkach są jasno przekazywane przed zatrudnieniem i/lub w ramach procedury wdrożenia nowego pracownika do pracy.
10. Szkolenie: Podmiot Przetwarzający zapewnia, by wszyscy pracownicy zostali właściwie poinformowani o mechanizmach kontroli bezpieczeństwa systemu IT, z którymi mają do czynienia w pracy. Pracownicy zajmujący się przetwarzaniem danych osobowych są ponadto odpowiednio informowani o odnośnych wymogach i obowiązkach prawnych w zakresie ochrony za pośrednictwem regularnych kampanii informacyjnych.
11. **Techniczne środki bezpieczeństwa**
    1. **Kontrola dostępu i uwierzytelnienie**
12. Wdrożono system kontroli dostępu stosowany do wszystkich użytkowników mających dostęp do systemu IT. System pozwala tworzyć, zatwierdzać, przeglądać i usuwać konta użytkowników.
13. Używanie wspólnych kont użytkowników nie jest zalecane. Jeśli jest to konieczne, zapewnia się, by wszyscy użytkownicy wspólnego konta mieli takie same funkcje i obowiązki.
14. W przypadku przyznawania dostępu lub przydzielania funkcji użytkownikom należy stosować zasadę „wiedzy koniecznej” w celu ograniczenia liczby użytkowników z dostępem do danych osobowych do tych użytkowników, dla których dostęp jest niezbędny, by zrealizować cele przetwarzania Podmiotu Przetwarzającego.
15. W przypadku gdy mechanizmy uwierzytelnienia wymagają hasła, Podmiot Przetwarzający zobowiązuje do stworzenia hasła składającego się z przynajmniej ośmiu znaków i spełniającego kryteria bardzo silnego hasła, w tym kryteria dotyczące długości, złożoności znaków i niepowtarzalności.
16. Dane uwierzytelniające (takie jak identyfikator i hasło użytkownika) nie mogą być przesyłane w sieci bez zabezpieczenia.
    1. **Rejestr zdarzeń i monitorowanie:** Pliki dziennika są aktywowane dla każdego systemu/programu stosowanego do przetwarzania danych osobowych. Obejmują wszystkie rodzaje dostępu do danych (przegląd, zmianę, usunięcie).
    2. **Bezpieczeństwo danych nieaktywnych**
17. **Bezpieczeństwo serwera/bazy danych**
    1. Bazy danych i serwery programów są skonfigurowane tak, aby działać przy użyciu odrębnego konta z minimalnymi uprawnieniami systemu operacyjnego umożliwiającymi poprawne działanie.
    2. Bazy danych i serwery programów przetwarzają jedynie dane osobowe, które są rzeczywiście konieczne do przetworzenia w celu realizacji celów przetwarzania.
18. **Bezpieczeństwo stanowiska pracy:**
    1. Użytkownicy nie są w stanie dezaktywować lub ominąć ustawień bezpieczeństwa.
    2. Programy antywirusowe oraz sygnatury zagrożeń są regularnie konfigurowane.
    3. Użytkownicy nie są uprawnieni do instalowania i dezaktywowania niezatwierdzonych programów.
    4. W systemie została aktywowana funkcja wygaszania sesji w przypadku braku aktywności użytkownika przez określony czas.
    5. Krytyczne aktualizacje zabezpieczeń wydawane przez twórcę systemu operacyjnego są regularnie instalowane.
    6. **Bezpieczeństwo sieci/komunikacji:**
19. W przypadku dostępu przez Internet komunikacja jest szyfrowana za pomocą protokołów kryptograficznych.
20. Dane przepływające do systemu IT i z systemu IT są monitorowane i kontrolowane poprzez zapory ogniowe i systemy wykrywania nieautoryzowanego dostępu.
    1. **Kopie zapasowe:**
21. Procedury dotyczące tworzenia kopii zapasowych i przywracania danych są opracowane, udokumentowane i wyraźnie przypisane do funkcji i obowiązków.
22. Poziom fizycznej i środowiskowej ochrony kopii zapasowych jest odpowiednio dostosowany do standardów obowiązujących w odniesieniu do danych źródłowych.
23. Tworzenie kopii zapasowych jest monitorowane w celu zapewnienia kompletności.
    1. **Urządzenia przenośne/mobilne:**
24. Procedury zarządzania urządzeniami mobilnymi i przenośnymi określające jasne zasady ich właściwego użycia są opracowane i udokumentowane.
25. Urządzenia mobilne, za pomocą których dozwolony jest dostęp do systemu informatycznego, są uprzednio rejestrowane i autoryzowane.
    1. **Bezpieczeństwo cyklu życia aplikacji:** Podczas cyklu rozwoju aplikacji stosuje się zatwierdzone standardy i praktyki bezpiecznego rozwoju oparte na aktualnym stanie wiedzy.
    2. **Usuwanie danych:**
26. Przed usunięciem nośników wykonane zostanie nadpisanie oparte na oprogramowaniu. Jeśli nie jest to możliwe, nośniki (płyty CD, DVD itp.) zostaną zniszczone fizycznie.
27. Dokumenty papierowe i przenośne nośniki używane do przechowywania danych osobowych są niszczone w niszczarce.
    1. **Bezpieczeństwo fizyczne:** Nieupoważniony personel nie ma dostępu do fizycznego obwodu infrastruktury systemu IT. W celu ochrony stref bezpieczeństwa i ich punktów dostępowych przed nieuprawionym dostępem należy zastosować odpowiednie środki techniczne (np. systemy wykrywania nieautoryzowanego dostępu, bramka z kołowrotkiem z czytnikiem kart chipowych, system kontroli wejścia, mechanizm zamykający) lub środki organizacyjne (np. pracownik ochrony).

**WYKONAWCA/ PODMIOT PRZETWARZAJĄCY**