

## Umowa powierzenia przetwarzania danych osobowych

zawarta w dniu .... 2026 r. pomiędzy

**Gminnym Zakładem Gospodarki Komunalnej Trzebnica – Ergo Spółka z o.o.**

ul. Milicka 23, 55-100 Trzebnica, wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego pod numerem KRS 000409746, NIP 9151788769, REGON: 021793317,  
zwaną w dalszej części umowy Administratorem Danych Osobowych lub Administratorem, reprezentowaną przez:

Marię Spalińską – Prezes Zarządu

Angelikę Szałąpską - Prokurenta

a

firmą: .....NIP ....., zwaną dalej „Podmiotem przetwarzającym”,  
w imieniu której działa:

.....

zwanymi łącznie „Stronami”, o następującej treści:

### § 1.

1. W związku z realizacją umowy nr ..... z dnia .....2026 r. (umowy głównej) Administrator Danych Osobowych powierza przetwarzanie danych osobowych Podmiotowi przetwarzającemu w trybie art. 28 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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), zwanym dalej RODO.
2. Administrator Danych Osobowych oświadcza, że, powierza dane Podmiotowi przetwarzającemu, w zakresie określonym w § 2
3. Powierzone dane zawierają informacje o osobach fizycznych.

### § 2.

1. Podmiot przetwarzający będzie przetwarzał wyłącznie dane osobowe, określone w Załączniku I, powierzone na podstawie niniejszej umowy, zwanej dalej Umową.
2. Szczegóły dotyczące operacji przetwarzania, w szczególności kategorie danych osobowych i cele, dla których dane osobowe są przetwarzane w imieniu Administratora, określono w Załączniku I.
3. Podmiot przetwarzający przetwarza dane osobowe wyłącznie w konkretnym celu lub celach przetwarzania, określonych w Załączniku I, chyba że otrzyma dalsze polecenia od Administratora.
4. Podmiot przetwarzający jest upoważniony do wykonywania czynności przetwarzania powierzonych danych wskazanych w Załączniku I, które są w minimalnym zakresie niezbędne do realizacji celów, o których mowa w ust. 2.



5. Podmiot przetwarzający będzie przetwarzał powierzone dane osobowe przez Administratora w siedzibie przetwarzającego.
6. Przetwarzanie przez Podmiot przetwarzający odbywa się wyłącznie przez okres określony w Załączniku I.

### § 3.

1. Podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane pisemne polecenie Administratora, chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo nie zabrania udzielenia takiej informacji z uwagi na ważny interes publiczny. Administrator może wydawać kolejne polecenia przez cały okres przetwarzania danych osobowych. Polecenia te są zawsze dokumentowane.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z Umową, Ustawą o ochronie danych osobowych i RODO oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. W celu zapewnienia bezpieczeństwa danych osobowych Podmiot przetwarzający wdraża co najmniej środki techniczne i organizacyjne określone w Załączniku II. Zapewnienie bezpieczeństwa danych obejmuje ochronę danych przed naruszeniem bezpieczeństwa prowadzącym do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych (naruszenie ochrony danych osobowych). Oceniając odpowiedni poziom bezpieczeństwa, Strony należyście uwzględniają stan wiedzy technicznej, koszty wdrażania, charakter, zakres, kontekst i cele przetwarzania oraz związane z tym ryzyko dla osób, których dane dotyczą.
4. Podmiot przetwarzający bezzwłocznie powiadamia Administratora, jeśli w opinii Podmiotu przetwarzającego polecenie wydane przez Administratora narusza RODO lub obowiązujące przepisy Unii lub państwa członkowskiego o ochronie danych.
5. Wszelkie decyzje dotyczące przetwarzania danych osobowych, odbiegające od ustaleń zawartych w Umowie, powinny być zaakceptowane przez Administratora w formie pisemnej (skan podpisanego pisma może być również przesłany drogą elektroniczną) pod rygorem ich nieważności.
6. Podmiot przetwarzający udziela członkom swojego personelu dostępu do danych osobowych podlegających przetwarzaniu jedynie w zakresie bezzwzględnie niezbędnym do wykonania umowy, zarządzania nią i jej monitorowania. Podmiot przetwarzający zapewnia, by osoby upoważnione do przetwarzania otrzymanych danych osobowych zobowiązały się do zachowania poufności lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania poufności.
7. Jeżeli przetwarzanie obejmuje dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne lub dane biometryczne do celów jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej danej osoby, bądź dane dotyczące wyroków skazujących i czynów



zabronionych („dane wrażliwe”), Podmiot przetwarzający stosuje szczególne ograniczenia lub dodatkowe zabezpieczenia.

#### § 4.

1. Podmiot przetwarzający niezwłocznie, nie później niż w terminie 5 dni, zawiadamia Administratora o prawnie umocowanym wniosku otrzymanym od osoby, której dane dotyczą. Podmiot przetwarzający nie odpowiada na taki wniosek, chyba że z przepisów prawa wynika zakaz zawiadomienia Administratora (w szczególności z przepisów postępowania karnego, gdy zakaz ma na celu zapewnienie poufności wszczętego dochodzenia).
2. Podmiot przetwarzający pomaga Administratorowi w wypełnianiu jego obowiązków dotyczących udzielania odpowiedzi na wnioski osób, których dane dotyczą, o skorzystanie z przysługujących im praw, z uwzględnieniem charakteru przetwarzania.
3. Wypełniając swoje obowiązki zgodnie z ust. 1 i 2, Podmiot przetwarzający stosuje się zawsze do poleceń Administratora.
4. Podmiot przetwarzający pomaga ponadto Administratorowi w zapewnieniu wypełniania następujących obowiązków (z uwzględnieniem charakteru przetwarzania danych oraz informacji, którymi dysponuje Podmiot przetwarzający):
  - a. obowiązek przeprowadzenia oceny wpływu planowanych operacji przetwarzania na ochronę danych osobowych („ocena skutków dla ochrony danych”), jeżeli dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych;
  - b. obowiązek skonsultowania się z właściwym(-i) organem(-ami) nadzorczym(-i) przed rozpoczęciem przetwarzania, jeżeli ocena skutków dla ochrony danych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby Administrator nie zastosował środków w celu jego ograniczenia;
  - c. obowiązek zapewnienia prawidłowości i aktualności danych osobowych poprzez niezwłoczne poinformowanie Administratora, jeżeli podmiot przetwarzający stwierdzi, że przetwarzane przez niego dane osobowe są nieprawidłowe lub nieaktualne;
  - d. obowiązki określone w art. 32 RODO.
5. W terminie 30 dni od zgłoszenia przez Administratora zapotrzebowania, Podmiot przetwarzający zobowiązuje się dostarczyć informacje i materiały:
  - a. do celów oceny skutków dla ochrony danych, o której mowa w art. 35 RODO
  - b. do konsultacji z Prezesem Urzędu ochrony Danych Osobowych, o której mowa w art. 36 RODO.
6. Strony określają w Załączniku II odpowiednie środki techniczne i organizacyjne, za pomocą których Podmiot przetwarzający jest zobowiązany pomagać Administratorowi w stosowaniu zapisów § 4, jak również zakres wymaganej pomocy.

#### § 5.

1. W przypadku naruszenia ochrony danych osobowych Podmiot przetwarzający współpracuje z Administratorem i pomaga mu w wypełnianiu jego obowiązków wynikających



z art. 33 i 34 RODO (z uwzględnieniem charakteru przetwarzania i informacji, którymi dysponuje Podmiot przetwarzający).

2. W przypadku naruszenia ochrony danych osobowych dotyczącego danych przetwarzanych przez Administratora, Podmiot przetwarzający zgłasza niezwłocznie naruszenie Administratorowi i wspomaga Administratora przy:

- 1) zgłaszaniu naruszenia ochrony danych osobowych właściwemu(-ym) organowi(-om) nadzorczemu(-ym) niezwłocznie po tym, jak Administrator dowiedział się o naruszeniu, w stosownych przypadkach/(chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych);
- 2) uzyskiwaniu następujących informacji, które zgodnie z art. 33 ust. 3 RODO powinny być zawarte w zgłoszeniu Administratora i obejmować co najmniej:
  - a) charakter danych osobowych, w tym w miarę możliwości kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
  - b) możliwe konsekwencje naruszenia ochrony danych osobowych;
  - c) środki zastosowane lub proponowane przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Jeżeli przekazanie wszystkich tych informacji równocześnie nie jest możliwe, pierwotne zgłoszenie zawiera informacje dostępne w danej chwili, a po uzyskaniu dostępu do dalszych informacji przekazuje się je bez zbędnej zwłoki;

- 3) wypełnianiu – zgodnie z art. 34 RODO – obowiązku zawiadomienia bez zbędnej zwłoki osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli naruszenie to może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych.
3. Podmiot przetwarzający zobowiązuje się niezwłocznie, nie później niż w terminie 7 godzin po stwierdzeniu naruszenia ochrony danych osobowych, zawiadomić Administratora o każdym takim naruszeniu - zgodnie z zasadami określonymi w art. 33 ust. 2 i 3 RODO.

## § 6.

1. Administrator ma prawo do kontroli sposobu wykonywania Umowy poprzez przeprowadzenie doraźnych kontroli dotyczących przetwarzania danych osobowych przez Podmiot przetwarzający oraz żądania składania przez niego pisemnych wyjaśnień.
2. Na zakończenie kontroli, o której mowa w ust. 1, przedstawiciel Administratora sporządza w 2 (dwóch) egzemplarzach protokół, który podpisują przedstawiciele obu Stron.
3. Podmiot przetwarzający może wnieść zastrzeżenia do protokołu w ciągu 5 dni roboczych od daty jego podpisania przez Strony.
4. Podmiot przetwarzający zobowiązuje się dostosować do zaleceń pokontrolnych mających na celu usunięcie uchybień i poprawę bezpieczeństwa przetwarzania danych osobowych.



5. Podmiot przetwarzający zobowiązuje się odpowiedzieć na każde pytanie Administratora dotyczące przetwarzania powierzonych mu na podstawie Umowy danych osobowych w terminie najpóźniej do 5 dni od dnia otrzymania pytania.
6. W przypadku gdy Podmiot przetwarzający narusza obowiązki wynikające z niniejszej Umowy i przepisów obowiązującego prawa, Administrator może polecić mu, by zawiesił przetwarzanie danych osobowych do czasu, gdy Podmiot przetwarzający zapewni zgodność z niniejszą Umową i przepisami obowiązującego prawa lub umowa ulega rozwiązaniu zgodnie z §11 ust. 1 pkt 3).
7. Podmiot przetwarzający zobowiązuje się niezwłocznie zawiadomić Administratora, jeżeli z jakiegokolwiek powodu nie jest w stanie zastosować się do niniejszej Umowy.

## **§ 7.**

1. Podmiot przetwarzający ma zgodę Administratora na korzystanie z usług podmiotów podprzetwarzających wpisanych do uzgodnionego wykazu, zgodnie z Załącznikiem III. Podmiot przetwarzający informuje Administratora na piśmie o wszelkich zamierzonych zmianach w tym wykazie polegających na dodaniu lub zastąpieniu podmiotów podprzetwarzających z wyprzedzeniem co najmniej 7 dni, dając tym samym Administratorowi czas na wyrażenie sprzeciwu wobec takich zmian przed rozpoczęciem korzystania z usług danego podmiotu podprzetwarzającego (podmiotów podprzetwarzających). Podmiot przetwarzający przekazuje Administratorowi niezbędne informacje.
2. Jeżeli Podmiot przetwarzający korzysta z usług podmiotu podprzetwarzającego w celu przeprowadzenia określonych czynności przetwarzania (w imieniu Administratora), dokonuje tego w drodze umowy, która nakłada na podmiot podprzetwarzający zasadniczo takie same obowiązki w zakresie ochrony danych jak obowiązki nałożone na Podmiot przetwarzający dane zgodnie z niniejszymi klauzulami. Podmiot przetwarzający zapewnia, aby podmiot podprzetwarzający wypełniał obowiązki, którym podlega Podmiot przetwarzający na mocy niniejszych klauzul oraz RODO.
3. Na wniosek Administratora Podmiot przetwarzający przekazuje Administratorowi kopię umowy, jaką zawarł z podmiotem podprzetwarzającym, a w razie wprowadzenia zmian przekazuje Administratorowi jej zaktualizowaną wersję. W zakresie niezbędnym do ochrony tajemnicy handlowej lub innych informacji poufnych, w tym danych osobowych, Podmiot przetwarzający może utajnić tekst umowy przed jej udostępnieniem.
4. Podmiot przetwarzający pozostaje w pełni odpowiedzialny przed Administratorem za wykonanie obowiązków podmiotu podprzetwarzającego zgodnie z jego umową z Podmiotem przetwarzającym i ponosi konsekwencje nieprawidłowego działania podmiotu podprzetwarzającego. Podmiot przetwarzający powiadamia Administratora o każdym przypadku niewywiązania się przez podmiot podprzetwarzający z jego zobowiązań umownych.
5. Podmiot przetwarzający uzgadnia z podmiotem podprzetwarzającym klauzulę dotyczącą beneficjenta będącego osobą trzecią, zgodnie z którą to klauzulą – jeżeli Podmiot przetwarzający przestanie istnieć faktycznie lub formalnie lub stanie się niewypłacalny – Administrator ma prawo rozwiązać umowę z podmiotem podprzetwarzającym i nakazać mu usunięcie lub zwrot danych osobowych.



## **§ 8.**

1. Wszelkie przekazywanie danych do państwa trzeciego lub organizacji międzynarodowej przez Podmiot przetwarzający odbywa się wyłącznie na udokumentowane polecenie Administratora lub w celu spełnienia szczególnego wymogu na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega Podmiot przetwarzający, i odbywa się zgodnie z rozdziałem V RODO.
2. Jeżeli Podmiot przetwarzający korzysta z usług podmiotu podprzetwarzającego w celu przeprowadzenia określonych czynności przetwarzania (w imieniu Administratora), które wiążą się z przekazywaniem danych osobowych w rozumieniu rozdziału V RODO, Administrator wyraża zgodę na to, by podmioty te mogły zapewnić zgodność z rozdziałem V RODO za pomocą standardowych klauzul umownych przyjętych przez Komisję Europejską zgodnie z art. 46 ust. 2 RODO, pod warunkiem że spełnione są warunki stosowania tych standardowych klauzul umownych.

## **§ 9.**

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy powierzonych mu przez Administratora Danych Osobowych i jest odpowiedzialny za ich udostępnienie lub wykorzystanie niezgodnie z Umową, a w szczególności za udostępnienie osobom nieupoważnionym.
2. W przypadku naruszenia przepisów Umowy, Ustawy o ochronie danych osobowych lub RODO przez Podmiot przetwarzający lub podprzetwarzający, w szczególności w następstwie którego Administrator Danych Osobowych, zostanie zobowiązany do wypłaty odszkodowania lub zostanie ukarany administracyjną karą pieniężną lub karą grzywny, Podmiot przetwarzający zobowiązuje się pokryć Administratorowi Danych Osobowych poniesione z tego tytułu straty i koszty (szkody).

## **§ 10.**

Umowa powierzenia zostaje zawarta na czas obowiązywania umowy głównej.

## **§ 11.**

1. Administrator ma prawo rozwiązać Umowę bez zachowania terminu wypowiedzenia, gdy Podmiot przetwarzający:
  - 1) wykorzystał dane osobowe w sposób niezgodny z Umową,
  - 2) powierzył przetwarzanie danych osobowych podprzetwarzającym z naruszeniem § 7,
  - 3) nie zaprzestał niewłaściwego przetwarzania danych osobowych w okresie zawieszenia ich przetwarzania i narusza swoje obowiązki wynikające z niniejszej Umowy, pomimo pisemnego wezwania do zaprzestania naruszeń i zapewnienia zgodności z niniejszą Umową.
  - 4) poważnie lub stale narusza niniejsze klauzule lub swoje obowiązki wynikające z RODO.
  - 5) nie wprowadził środków zabezpieczających w celu zaradzenia naruszeniu ochrony danych osobowych, w tym o których mowa w art. 33 ust. 3 lit. d RODO.
  - 6) zawiadomi o swojej niezdolności do dalszego wykonywania Umowy.
  - 7) nie stosuje się do wiążącej decyzji właściwego sądu lub właściwego(-ych) organu(-ów) nadzorczego(-ych) dotyczącej jego obowiązków wynikających z niniejszej umowy lub z RODO.



2. Podmiot przetwarzający ma prawo rozwiązać Umowę w zakresie, w jakim dotyczy ona przetwarzania danych osobowych zgodnie z niniejszą umową jeżeli po zawiadomieniu Administratora o tym, że jego polecenie narusza obowiązujące wymogi prawne zgodnie z §3 ust. 4 Umowy, Administrator nalega na wypełnienie polecenia.

#### **§ 12.**

1. Podmiot przetwarzający, w przypadku wygaśnięcia Umowy niezwłocznie, ale nie później niż w terminie 5 dni kalendarzowych, zobowiązuje się zwrócić lub usunąć – zależnie od decyzji Administratora Danych Osobowych - wszelkie dane osobowe oraz wszelkie ich istniejące kopie, których przetwarzanie zostało mu powierzone, w tym również z nośników elektronicznych pozostających w jego dyspozycji i potwierdzić powyższe przekazaniem Administratorowi Danych Osobowych protokołem, chyba że prawo Unii lub prawo państwa członkowskiego nakazuje przechowywanie danych osobowych.
2. Podmiot przetwarzający zobowiązany jest złożyć razem z protokołem, o którym mowa w ust. 1, pisemne oświadczenie, że powierzone dane osobowe, po zakończeniu umowy: trwale usunął i nie przetwarza powierzonych danych w rozumieniu art. 4 pkt 2 RODO.

#### **§ 13.**

Wszelkie zmiany Umowy wymagają formy pisemnej pod rygorem nieważności.

#### **§ 14.**

W sprawach nieuregulowanych w Umowie mają zastosowanie przepisy Ustawy o ochronie danych osobowych, RODO i Kodeksu Cywilnego oraz innych obowiązujących przepisów prawa, a także postanowienia umowy, o której mowa w § 1 ust. 1.

#### **§ 15.**

Spory wynikłe z tytułu Umowy będzie rozstrzygał Sąd właściwy dla miejsca siedziby Administratora Danych Osobowych.

#### **§ 16.**

Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

.....  
(Administrator Danych)  
Osobowych

.....  
(Podmiot przetwarzający)



## ZAŁĄCZNIK I

### 1. Opis przetwarzania

- Kategorie osób, których dane osobowe są przetwarzane:

pracownicy Administratora, klienci Administratora *(niepotrzebne skreślić/usunąć, brakujące dopisać)*

- Kategorie przetwarzanych danych osobowych

imię i nazwisko, dane kontaktowe (adres zamieszkania, adres e-mail, numer telefonu), data urodzenia, miejsce urodzenia i inne dane szczególnych kategorii, które mogą zostać przekazane przez klienta Administratorowi w treści składanych dokumentów lub wpisane w metrykach rejestrowanych w systemie dokumentów (np. PESEL, NIP)

*(niepotrzebne skreślić/usunąć, brakujące dopisać)*

- dane szczególne (wrażliwe) brak..... *(należy wymienić)*
- stosowane ograniczenia lub zabezpieczenia, które w pełni uwzględniają charakter danych i związane z nimi zagrożenia:

- ścisłe ograniczenie celu,
- ograniczenia dostępu (w tym dostęp wyłącznie dla personelu, który odbył specjalistyczne szkolenie),
- prowadzenie rejestru dostępu do danych,
- ograniczenia dotyczące dalszego przekazywania danych,
- monitoring budynku
- kontrola dostępu do budynku (ochrona, portiernia, szlaban)
- kontrola dostępu do pomieszczeń biurowych (czytnik kart magnetycznych, kod do drzwi)
- dokumentacja zawierająca dane osobowe przechowywana w zamykanych meblach
- dostęp do każdego z urządzeń zabezpieczony jest loginem i hasłem znanym jedynie osobom posiadającym upoważnienie do przetwarzania danych osobowych
- oświadczenia pracowników o poufności
- wewnętrzne procedury ściśle określające zasady korzystania z systemów



- szyfrowane połączenia sieciowe
- zabezpieczanie plików z danymi osobowymi do ZIP z hasłem wysyłanym inną drogą komunikacji niż sam plik
- audyt i zbieranie logów dostępu użytkowników do systemów
  - Charakter przetwarzania
    - system informatyczny

*(niepotrzebne skreślić/usunąć, brakujące dopisać)*

- Cel(e), w którym(-ych) dane osobowe są przetwarzane w imieniu Administratora realizacji Umowy głównej

*(niepotrzebne skreślić/usunąć, brakujące dopisać)*

- Czas trwania przetwarzania:  
czas trwania umowy *(niepotrzebne skreślić/usunąć, brakujące dopisać)*

- Czynności przetwarzania:  
przechowywanie, przeglądanie, wykorzystywanie *(niepotrzebne skreślić, brakujące dopisać)*

**Opis przetwarzania w przypadku przetwarzania przez podmioty podprzetwarzające (nie dotyczy):**

- Kategorie osób, których dane osobowe są przetwarzane: (nie dotyczy)  
*(niepotrzebne skreślić/usunąć, brakujące dopisać)*
- Kategorie przetwarzanych danych osobowych (nie dotyczy)  
*(niepotrzebne skreślić/usunąć, brakujące dopisać)*
- dane szczególne (wrażliwe)..... *(należy wymienić)* (nie dotyczy)
- stosowane ograniczenia lub zabezpieczenia, które w pełni uwzględniają charakter danych i związane z nimi zagrożenia (nie dotyczy)
- Czas trwania przetwarzania (nie dotyczy)
- Czynności przetwarzania (nie dotyczy)



*(niepotrzebne skreślić/usunąć, brakujące dopisać)*

## ZAŁĄCZNIK II

Środki techniczne i organizacyjne, w tym środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa danych

Opis technicznych i organizacyjnych środków bezpieczeństwa wdrożonych przez podmiot przetwarzający (podmioty przetwarzające) (w tym wszelkie stosowne certyfikaty) w celu zapewnienia odpowiedniego poziomu bezpieczeństwa, z uwzględnieniem charakteru, zakresu, kontekstu i celu przetwarzania, a także ryzyka naruszenia praw i wolności osób fizycznych:

- Środki umożliwiające pseudonimizację i szyfrowanie danych osobowych

Kwestia pseudonimizacji danych osobowych w Systemie Informacji Przestrzennej w całości zależy od Administratora Danych Osobowych. Musi istnieć możliwość szyfrowania danych podczas ich przechowywania i transmisji z zapewnieniem wyłącznej kontroli przez Administratora usług nad procesami generowania i zarządzania kluczami.

*(niepotrzebne skreślić/usunąć, brakujące dopisać)*

- Środki zapewniające zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania

W organizacji funkcjonuje szereg procedur: m.in. Analiza ryzyka, Polityka Bezpieczeństwa, Instrukcja Zarządzania Systemem Informatycznym, Polityka prywatności, które zapewniają wspomnianą zdolność.

*(niepotrzebne skreślić/usunąć, brakujące dopisać)*

- Środki zapewniające zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego

Organizacja posiada plany ciągłości działania mające na celu zapewnić maksymalną dostępność. W razie problemów posiada możliwość szybkiego przywrócenia dostępności w środowisku awaryjnym.

*(niepotrzebne skreślić/usunąć, brakujące dopisać)*

- Procesy umożliwiające regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania

Zabezpieczenia stosowane w oparciu o analizę ryzyka, która jest procesem stałym a nie działaniem jednorazowym.



Przeprowadzanie audytu wewnętrznego dotyczącego zasad bezpieczeństwa informacji, w tym danych osobowych, w celu weryfikacji spełnienia wymogów polityki ochrony danych.

*(niepotrzebne skreślić/usunąć, brakujące dopisać)*

- Środki umożliwiające identyfikację i autoryzację użytkowników

W systemie wszyscy użytkownicy posługują się imiennymi kontami. Operacje wykonywane przez użytkowników są logowane.

*(niepotrzebne skreślić/usunąć, brakujące dopisać)*

- Środki zapewniające ochronę danych w czasie ich przekazywania

Dane przesyłane pomiędzy systemem a urządzeniem klienta szyfrowane są za pomocą protokołu SSL, zapewniającym integralność i poufność komunikacji

*(niepotrzebne skreślić/usunąć, brakujące dopisać)*

- Środki zapewniające ochronę danych w czasie ich przechowywania

Dostęp do danych w bazie zabezpieczony poprzez mechanizm autoryzacji, realizowany na poziomie DBMS. Dostęp do danych w bazie ograniczony jest jedynie do klienta aplikacyjnego. Dostęp do plików realizowany jest na poziomie autoryzacji dostępu do sieciowego systemu plików opartego na redundantnych dyskach twardych zapewniających ich zabezpieczenie przed uszkodzeniem i degradacją.

*(niepotrzebne skreślić/usunąć, brakujące dopisać)*

- Środki służące zapewnieniu bezpieczeństwa fizycznego miejsc, w których przetwarzane są dane osobowe

Dostęp do pomieszczeń organizacji tylko dla osób uprawnionych – pomieszczenia zabezpieczone zamkami w drzwiach do pomieszczeń biurowych (kody dostępów), wejście na korytarz przy użyciu karty zbliżeniowej. Obiekt zabezpieczony monitoringiem wizyjnym i dozorem firmy ochroniarskiej.

*(niepotrzebne skreślić/usunąć, brakujące dopisać)*

- Środki umożliwiające rejestrowanie zdarzeń

Zdarzenia i błędy aplikacji logowane są za pomocą mechanizmu logów systemowych.

*(niepotrzebne skreślić/usunąć, brakujące dopisać)*

- Środki służące do konfiguracji systemu, w tym konfiguracji domyślnej



Konfiguracja systemu realizowana jest zgodnie z wymaganiami konfiguracyjnymi aplikacji.

*(niepotrzebne skreślić/usunąć, brakujące dopisać)*

- Środki dotyczące zarządzania wewnętrznym systemem IT i bezpieczeństwem IT

W organizacji funkcjonuje Polityka Bezpieczeństwa oraz Instrukcja zarządzania systemem informatycznym.

*(niepotrzebne skreślić/usunąć, brakujące dopisać)*

- Środki dotyczące certyfikacji / zapewnienia jakości procesów i produktów:

W organizacji przeprowadzane są audyty wewnętrzne dotyczące zasad bezpieczeństwa informacji

*(niepotrzebne skreślić/usunąć, brakujące dopisać)*

- Środki zapewniające minimalizację danych

Zakres danych przetwarzanych w Systemie Informacji Przestrzennej zależy od Administratora. Organizacja przetwarza dane w zakresie niezbędnym do realizacji umowy wsparcia i utrzymania systemu – dane pozyskiwane od Administratora .

*(niepotrzebne skreślić/usunąć, brakujące dopisać)*

- Środki zapewniające odpowiednią jakość danych

Zakres danych przetwarzanych w Systemie Informacji Przestrzennej zależy od Administratora. Organizacja przetwarza dane w zakresie niezbędnym do realizacji umowy wsparcia i utrzymania systemu – dane pozyskiwane od Administratora .

*(niepotrzebne skreślić/usunąć, brakujące dopisać)*

- Środki zapewniające ograniczone zatrzymywanie danych

Zgodnie z zapisami umowy.

*(niepotrzebne skreślić/usunąć, brakujące dopisać)*

- Środki zapewniające rozliczalność

Logowanie operacji wykonywanych na danych wraz informacją o tym kto, kiedy i jakie operacje na danych osobowych przeprowadzał. Procedury obowiązujące w organizacji regulują kwestię przetwarzania danych tylko na polecenie Administratora Danych Osobowych.

*(niepotrzebne skreślić/usunąć, brakujące dopisać)*



- Środki umożliwiające przenoszenie danych i zapewnienie ich usuwania

Przeniesienie/usuwanie danych – zgodnie z dyspozycją Administratora, jeśli zaistnieje taka potrzeba. *(niepotrzebne skreślić/usunąć, brakujące dopisać)*

Opis konkretnych środków technicznych i organizacyjnych, jakie powinien zastosować podmiot przetwarzający, aby móc udzielić pomocy Administratorowi (wymienić i opisać konkretne środki):

1. Identyfikacja użytkownika, który wykonywał w danym okresie działania na danych.
2. Udostępnienie danych z monitoringu lub danych z systemów pozwalających zidentyfikować osoby, które przebywały w pomieszczeniach i mogły mieć dostęp do danych w określonym czasie.
3. Informacja o czasie zdarzenia i błędach jakie pojawiły się w danym czasie w aplikacji.
4. Informacja jakie działania (operacje) były wykonywane na danych wraz informacją o tym kto, kiedy je przeprowadzał.
5. Informacja o czasie i zachowaniach anomalnych aplikacji w danym okresie.
6. Udostępnienie Procedury zarządzania incydentami.
7. Korelacja danych i utworzenie raportu o incydencie.
8. Analiza śledcza danego zdarzenia.

*(niepotrzebne skreślić/usunąć, brakujące dopisać)*



ZAŁĄCZNIK III - nie dotyczy

### Wykaz podmiotów podprzetwarzających

Niniejszy załącznik należy wypełnić w razie udzielenia szczegółowej zgody na korzystanie z usług podmiotów podprzetwarzających.

Administrator zezwolił na korzystanie z usług następujących podmiotów podprzetwarzających:

1. Imię nazwisko lub nazwa

.....

• Adres

.....

• imię i nazwisko, stanowisko i dane kontaktowe osoby wyznaczonej do kontaktów:

.....

• Opis przetwarzania (w tym jasne określenie zakresu odpowiedzialności w przypadku upoważnienia kilku podmiotów podprzetwarzających):

.....

2. Imię nazwisko lub nazwa

.....

• Adres

.....

• imię i nazwisko, stanowisko i dane kontaktowe osoby wyznaczonej do kontaktów:

.....

• Opis przetwarzania (w tym jasne określenie zakresu odpowiedzialności w przypadku upoważnienia kilku podmiotów podprzetwarzających):

.....