Uchwała nr XLVI/207/I/2024
Zarządu Związku Powiatowo-Gminnego
„Wielkopolski Transport Regionalny"
z dnia 4 marca 2024 roku

w sprawie:
przyjęcia Polityki Bezpieczeństwa Ochrony Danych Osobowych Związku Powiatowo-Gminnego „Wielkopolski Transport Regionalny"

Na podstawie § 27 ust. 1 i 3 statutu Związku Powiatowo-Gminnego „Wielkopolski Transport Regionalny" (Dziennik Urzędowy Województwa Wielkopolskiego z 2024 r., poz. 1025) uchwala się, co następuje:

§ 1.

Przyjmuje się Politykę Bezpieczeństwa Ochrony Danych Osobowych Związku Powiatowo-Gminnego „Wielkopolski Transport Regionalny" w brzmieniu stanowiącym załącznik do niniejszej uchwały.

§ 2.

Wykonanie uchwały powierza się Zarządowi oraz Dyrektorowi Biura Związku.

§ 3.

Uchwała wchodzi w życie z dniem podjęcia.

Zarząd Związku Powiatowo-Gminnego „Wielkopolski Transport Regionalny"

Piotr Hojan	**Przewodniczący**	.....
Tomasz Łubiński	**Zastępca Przewodniczącego**	.....
Adam Lewandowski	**Zastępca Przewodniczącego**	.....
Andrzej Wilkoński	**Członek Zarządu**	.....
Paweł Adam	**Członek Zarządu**	.....

Załącznik do uchwały Zarządu Związku Powiatowo-Gminnego „Wielkopolski Transport Regionalny" nr XLVI/208/I/2024 z dnia 4 marca 2024 roku

Polityka Bezpieczeństwa Ochrony Danych Osobowych

Związek Powiatowo-Gminny

„Wielkopolski Transport Regionalny" w Poznaniu

Zakres dostępu do dokumentu:

1. Administrator Danych
2. Inspektor Ochrony Danych
3. Główny Administrator Bezpieczeństwa Systemów
4. Pracownicy

Zakres dostępu do dokumentu:

1. Wszystkie osoby zaangażowane w przetwarzanie danych osobowych
2. Podmioty i instytucje upoważnione na podstawie przepisów prawa

Spis treści

1. POSTANOWIENIA OGÓLNE

1.1. Polityka Bezpieczeństwa Ochrony Danych Osobowych została opracowana i wdrożona w strukturze Administratora Danych Osobowych – Związku Powiatowo-Gminnego „Wielkopolski Transport Regionalny" z siedzibą w Poznaniu w celu zapewnienia zgodności przetwarzania danych osobowych z uwzględnieniem:

1) wymogów powszechnie obowiązujących europejskich i polskich przepisów prawa związanych z ochroną danych osobowych i bezpieczeństwem informacji, w szczególności:
   - Rozporządzeniem 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),
   - Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych;
2) wytycznych Prezesa Urzędu Ochrony Danych Osobowych i innych organów zaangażowanych w ochronę danych osobowych;
3) dobrych praktyk, wytycznych lub standardów branży lub sektora, który reprezentuje Administrator Danych Osobowych.

1.2. Polityka Bezpieczeństwa Ochrony Danych Osobowych służy zapewnieniu takiego poziomu bezpieczeństwa przetwarzanych przez Administratora Danych Osobowych danych osobowych, który uchroni je przed:

1) dostępem osób nieupoważnionych,
2) nieuprawnioną zmianą, utratą, uszkodzeniem lub zniszczeniem.

1.3. Polityka Bezpieczeństwa Ochrony Danych Osobowych jest poddawana okresowym przeglądom. W razie potrzeby dokonuje się stosownych zmian jej treści, przy uwzględnieniu w szczególności:

1) przepisów lub wytycznych, o których mowa w ust. 1.1 powyżej,
2) aktualnego stanu wiedzy technicznej,
3) możliwości logistycznych, kadrowych i finansowych Administratora Danych Osobowych.

1.4. Polityka Bezpieczeństwa Ochrony Danych Osobowych jest wewnętrznym dokumentem Administratora Danych Osobowych i ma zastosowanie do wszystkich nowo przyjętych pracowników, stażystów, praktykantów jak i do zatrudnionych pracowników Administratora Danych Osobowych, którzy w zakresie swoich obowiązków przetwarzają dane osobowe, jak również innych osób, które z upoważnienia Administratora Danych Osobowych uzyskały dostęp do danych osobowych.

1.5. Każda z ww. osób została zapoznana z najważniejszymi procedurami bezpieczeństwa danych opisanymi w Polityce Bezpieczeństwa Ochrony Danych Osobowych i zobowiązana do ich

przestrzegania w zakresie wynikającym z przydzielonych zadań. Osoby, o których mowa złożyły oświadczenie o zapoznaniu się z procedurami bezpieczeństwa danych oraz zobowiązały się do ich stosowania.

1.6. Treść Polityki Bezpieczeństwa Ochrony Danych Osobowych nie może być udostępniana osobom lub podmiotom nieupoważnionym.

1.7. Integralną część Polityki Bezpieczeństwa Ochrony Danych Osobowych stanowią załączniki do niej, wskazane w rozdziale 11. Ponadto Administrator Danych Osobowych może wprowadzać - lub dopuszczać do stosowania - dodatkowe wytyczne, regulaminy i instrukcje, mające na celu realizację zasad ochrony danych osobowych i bezpieczeństwa informacji, opisanych w Polityce Bezpieczeństwa Ochrony Danych Osobowych.

2. PODSTAWOWE POJĘCIA

Określenia użyte w Polityce Bezpieczeństwa Ochrony Danych Osobowych oznaczają:

2.1. **RODO** - Rozporządzenie 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)

2.2. **USTAWA** - Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. 2019r. poz. 1781)

2.3. **PBDO / Polityka bezpieczeństwa** - Polityka Bezpieczeństwa Ochrony Danych Osobowych

2.4. **PBI** - Polityka Bezpieczeństwa Informacji

2.5. **AD / Administrator / Administrator Danych Osobowych** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. W rozumieniu Polityki bezpieczeństwa AD jest Związek Powiatowo-Gminny „Wielkopolski Transport Regionalny" z siedzibą w Poznaniu

2.6. **ABS** - Administrator Bezpieczeństwa Systemów

2.7. **Biuro** – siedziba Administratora Danych Osobowych mieszcząca się przy ul. Zielonej 8 w Poznaniu

2.8. **IOD** - Inspektor Ochrony Danych, będący osobą wspierającą AD w realizacji obowiązków wynikających z przepisów o ochronie danych osobowych

2.9. **Zastępca IOD** - Zastępca Inspektora Ochrony Danych, zastępujący IOD w czasie jego nieobecności

2.10. **Osoba upoważniona** - osoba posiadająca upoważnienie do przetwarzania danych osobowych (pracownik, stażysta, praktykant, inne osoby)

2.11. **RCPD** - Rejestr Czynności Przetwarzania Danych Osobowych, o którym mowa w art. 30 ust. 1

RODO

2.12. **RKCPD** - Rejestr Kategorii Czynności Przetwarzania Danych Osobowych, o którym mowa w art. 30 ust. 2 RODO

2.13. **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

2.14. **Szczególne kategorie danych osobowych** - informacje o osobie fizycznej dotyczące pochodzenia rasowego lub etnicznego, poglądów politycznych, przekonań religijnych lub światopoglądowych, przynależności do związków zawodowych, przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby

2.15. **Prezes UODO** – Prezes Urzędu Ochrony Danych Osobowych będący organem właściwym do spraw ochrony danych osobowych w Polsce, organ nadzorczy w rozumieniu RODO

2.16. **Obszar przetwarzania danych osobowych** – teren, na którym AD dokonuje przetwarzania danych osobowych w formie papierowej lub elektronicznej

2.17. **Naruszenie / naruszenie ochrony danych osobowych** - naruszenie bezpieczeństwa danych osobowych prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych

2.18. **Przetwarzanie** - operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka 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

2.19. **Podmiot przetwarzający (procesor)** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu AD

2.20. **Profilowanie** - dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji,

zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się

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

2.22. **Odbiorca** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców. Przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania

2.23. **Strona trzecia** - osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które z upoważnienia administratora lub podmiotu przetwarzającego - mogą przetwarzać dane osobowe.

3. OCHRONA DANYCH OSOBOWYCH W ZWIĄZKU POWIATOWO-GMINNYM „WIELKOPOLSKI TRANSPORT REGIONALNY" W POZNANIU

3.1. Utrzymanie bezpieczeństwa informacji przetwarzanych w Związku Powiatowo-Gminnym „Wielkopolski Transport Regionalny", w tym danych osobowych rozumiane jest jako zapewnienie ich poufności, integralności i rozliczalności na odpowiednim poziomie.

3.2. Realizując PBDO Związek Powiatowo-Gminny „Wielkopolski Transport Regionalny" stosuje następujące zasady przetwarzania danych osobowych:

1) **zgodność z prawem, rzetelność i przejrzystość** - dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą,
2) **ograniczenie celu** - dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami. Dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 RODO za niezgodne z pierwotnymi celami,
3) **minimalizacja danych** - dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane,
4) **prawidłowość** - dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane. Należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane,
5) **ograniczenie przechowywania** - dane osobowe muszą być 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. Dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 RODO z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy RODO w celu ochrony praw i wolności osób, których dane dotyczą,

6) **integralność i poufność** - dane osobowe muszą być 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,

7) **rozliczalność** - AD jest odpowiedzialny za przestrzeganie zasad zawartych w ust. 3.2 powyżej i musi być w stanie wykazać ich przestrzeganie.

3.3. Dostęp do danych osobowych mogą mieć tylko osoby posiadające upoważnienie do ich przetwarzania.

3.4. Przebywanie osób nieuprawnionych do przetwarzania danych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania, chyba, że dane te są w odpowiedni sposób zabezpieczone przed dostępem.

3.5. Osoby mające dostęp do danych osobowych nie mogą ich ujawniać osobom nieuprawnionym zarówno w miejscu ich przetwarzania, jak i poza nim oraz zobowiązani są do ich zabezpieczenia w sposób uniemożliwiający dostęp przez osoby nieuprawnione.

3.6. Niedopuszczalne jest wynoszenie dokumentów niezależnie od sposobu ich wytworzenia oraz innych nośników zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada osoba dokonująca ich wyniesienia.

3.7. Wysyłanie seryjnych wiadomości e-mail wymaga zastosowania opcji *kopia ukryta (ukryte do wiadomości).*

3.8. Nie można udzielać informacji dotyczących danych osobowych innym podmiotom na podstawie prośby o takie dane skierowane w formie zapytania telefonicznego, za wyjątkiem sytuacji prawem przepisanych. Udzielając informacji drogą telefoniczną należy podjąć wszelkie możliwe działania mające na celu właściwą identyfikację tożsamości rozmówcy.

3.9. W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. *„czystego biurka”,* która oznacza niepozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieupoważnionym. Za realizację powyższej zasady odpowiedzialny jest na swym

stanowisku każdy z pracowników. Nie należy pozostawiać danych osobowych w miejscach ogólnodostępnych takich jak np. biurka, blaty, parapety, drukarki, skanery, urządzenia wielofunkcyjne.

3.10. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe odbywać się musi w sposób uniemożliwiający odczytanie zawartej w nich treści, w szczególności z wykorzystaniem niszczarek.

3.11. Za bezpieczeństwo przetwarzania danych w określonym zbiorze indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik lub inna osoba mająca dostęp do danych.

3.12. W czasie chwilowej nieobecności pracowników w pomieszczeniach, w godzinach pracy jak i po zakończeniu pracy, są oni zobowiązani do zamykania na klucz pomieszczeń wchodzących w skład obszarów, w których przetwarzane są dane osobowe, a także blokowania systemu teleinformatycznego.

3.13. Po zakończeniu pracy w systemie informatycznym, w którym przechowywane są dane osobowe, należy się wylogować z systemu.

3.14. Na pracowniku wykonującym pracę zdalną spoczywa obowiązek odpowiedniego zabezpieczenia danych tak, aby osoby trzecie nie miały dostępu do danych osobowych.

3.15. Dane osobowe przesyłane elektronicznie powinny być zabezpieczone hasłem. Hasło to powinno być wysyłane oddzielnym kanałem telekomunikacyjnym, z uwzględnieniem szyfrowania nośników i danych.

4. ZASADY STOSOWANIA

4.1. Zasady PBDO obejmują cały system przetwarzania danych osobowych w Związku Powiatowo-Gminnym „Wielkopolski Transport Regionalny" z siedzibą w Poznaniu, a w szczególności:

- wszystkie istniejące, wdrażane obecnie i w przyszłości systemy informatyczne oraz dokumenty papierowe zawierające dane osobowe,
- informacje dotyczące zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach informatycznych przetwarzających dane osobowe oraz innych dokumentów zawierających dane osobowe,
- wszystkie dokumenty oraz nośniki elektroniczne, magnetyczne lub optyczne zawierające dane osobowe podlegające ochronie,
- wszystkie lokalizacje – w szczególności pomieszczenia Biura, w których są lub będą przetwarzane dane osobowe,
- wszystkich pracowników w rozumieniu przepisów Kodeksu pracy, praktykantów,

stażystów i innych osób mających dostęp do danych osobowych.

4.2. Administrator w zakresie przetwarzanych przez siebie danych osobowych dopuszcza możliwość przyjęcia modelu współadministrowania danymi osobowymi zgodnie z art. 26 RODO.

4.3. Zasady współadministrowania są określane w odrębnym dokumencie na drodze wspólnych uzgodnień, w przejrzysty sposób określający odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO.

4.4. Administrator realizując PBDO, w zakresie udostępniania danych osobowych w ramach własnej (wewnętrznej) struktury, zezwala na ich przetwarzanie w systemie informatycznym lub w wersji papierowej wyłącznie osobom, które uzyskały uprzednie, stosowne upoważnienie do przetwarzania danych osobowych.

4.5. Upoważnienie do przetwarzania danych osobowych nadawane jest po przeprowadzeniu szkolenia, osoby upoważnionej.

4.6. Upoważnienie do przetwarzania danych osobowych, nadawane jest indywidualnie, z wyraźnym wskazaniem, jakie zbiory danych i zasoby obejmuje swoim zakresem. Wzór upoważnienia stanowi załącznik nr 1 do PBDO.

4.7. Upoważnienie wydawane jest w 2 egzemplarzach, w tym jeden dla Administratora, który jest przekazywany do rejestru upoważnień do przetwarzania danych oraz drugi dla osoby szkolonej. Kopia upoważnienia zostaje dostarczona na stanowisko do obsługi kadr i płac celem dołączenia go do akt osobowych. IOD również przechowuje kopie wydanych upoważnień.

4.8. W przypadku firm zewnętrznych świadczących usługi na rzecz Związku Powiatowo – Gminnego „Wielkopolski Transport Regionalny" osoba upoważniona przez AD oraz przedstawiciel firmy zewnętrznej zgłaszają osoby świadczące usługi na terenie Biura do IOD, celem przeszkolenia (w przypadku pracowników ochrony) i wystawienia upoważnienia oraz oświadczenia o zachowaniu poufności informacji chronionych oraz przebywania w pomieszczeniach, gdzie znajdują się dane osobowe. Wzór oświadczenia stanowi załącznik nr 2 do PBDO.

4.9. Administrator realizując PBDO oraz swoje zadania wynikające z przepisów prawa, dopuszcza by dane osobowe, których jest administratorem były przekazywane innym administratorom w formie udostępnienia danych.

4.10. Udostępnienie danych może nastąpić tylko w oparciu o co najmniej jedną przesłankę spośród wskazanych w art. 6 RODO i / lub art. 9 RODO.

4.11. Osoby upoważnione do przetwarzania danych, które w ramach swych obowiązków służbowych udostępniają dane osobowe, mają obowiązek prowadzić ewidencję

udostępnianych danych, która znajduje się w rejestrze Biura oraz stosować się do Schematu udostępniania danych, stanowiącego załącznik nr 3 do PBDO.

4.12. Przekazanie danych powinno odbywać się w bezpieczny sposób z poszanowaniem m.in. zasad integralności i poufności.

4.13. Administrator realizując PBDO oraz swoje zadania wynikające z przepisów prawa dopuszcza, by dane osobowe, których jest administratorem były przetwarzane poza własnymi strukturami organizacyjnymi. Może się to odbywać wyłącznie na drodze powierzenia danych, w określonym celu i zakresie, podmiotowi przetwarzającemu na mocy umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego, zgodnie z art. 28 ust. 3 RODO.

4.14. Osoby odpowiedzialne za przygotowanie umowy powierzenia, zobowiązane są poinformować o tym IOD oraz skonsultować z nim postanowienia zawieranej umowy w zakresie powierzenia przetwarzania danych osobowych. Powierzenie przetwarzania danych może odbywać się wyłącznie na podstawie postanowień zaakceptowanych przez IOD.

4.15. Umowa powierzenia przetwarzania danych osobowych podpisywana jest zgodnie z zasadami reprezentacji Administratora lub udzielonymi pełnomocnictwami.

4.16. Każdorazowe dokonanie powierzenia danych osobowych musi zostać odnotowane w rejestrze umów.

4.17. Osoby odpowiedzialne za przygotowanie umowy, w których projektowane są postanowienia dotyczące danych osobowych, a nie stanowiącymi umowy powierzenia zgodnie z ust. 4.13 powyżej, zobowiązane są poinformować o tym IOD oraz skonsultować z nim postanowienia zawieranej umowy w zakresie ochrony danych osobowych. Postanowienia o którym mowa w zdaniu pierwszym muszą zostać zaakceptowane przez IOD.

4.18. Administrator w zakresie prowadzonej przez siebie działalności może przetwarzać również dane osobowe powierzone mu przez podmioty, na rzecz których świadczy usługi. Przyjęcie danych w powierzenie przez Administratora musi zostać odnotowane w prowadzonym rejestrze umów.

4.19. Związek Powiatowo – Gminny „Wielkopolski Transport Regionalny" prowadzi archiwum dokumentów papierowych i informatycznych zawierających dane osobowe w wydzielonych do tego celu i zabezpieczonych pomieszczeniach.

4.20. Administrator uwzględnia w zachodzących w jego strukturze procesach przetwarzania danych osobowych, zasady ułatwiające osobie, której dane dotyczą, wykonywanie praw przysługujących jej na mocy przepisów RODO, w tym w szczególności:

- Prawo do wycofania wyrażonej zgody (art. 7 ust. 3 RODO),
- Prawo dostępu przysługujące osobie, której dane dotyczą (art. 15 RODO),

- Prawo do sprostowania danych (art. 16 RODO),
- Prawo do usunięcia danych (prawo do bycia zapomnianym) (art. 17 RODO),
- Prawo do ograniczenia przetwarzania (art. 18 RODO),
- Prawo do przenoszenia danych (art. 20 RODO),
- Prawo do sprzeciwu (art. 21 RODO),
- Prawo do niepodlegania decyzjom opartym na zautomatyzowanym przetwarzaniu (art. 22 RODO).

4.21. W Biurze oraz w innych miejscach prowadzenia działalności przez AD obowiązki informacyjne realizowane są zgodnie z art. 13 i 14 RODO. Za spełnianie obowiązku informacyjnego odpowiadają kierujący komórkami organizacyjnymi AD, jak również osoby zajmujące stanowiska samodzielne. Realizacja obowiązków informacyjnych wynikających z przepisów prawa, należy do osoby prowadzającej sprawę.

4.22. Obowiązki informacyjne są konsultowane z IOD.

5. INCYDENTY NARUSZENIA OCHRONY DANYCH OSOBOWYCH

5.1. Osoby upoważnione do przetwarzania danych osobowych są zobowiązane do szczególnej staranności przy przetwarzaniu danych osobowych.

5.2. Każdorazowo przed przystąpieniem do pracy są zobowiązani do dokonania oceny i oględzin miejsca pracy pod kątem, czy nie dokonano jakichkolwiek nieuprawnionych działań związanych z ochroną danych osobowych przez osoby nieuprawnione.

5.3. W sytuacji, gdy stwierdzą incydent naruszenia lub próby naruszenia ochrony danych osobowych, wówczas są zobowiązani do niezwłocznego poinformowania o tym fakcie przełożonego / IOD / Administratora.

5.4. Osoba zgłaszająca incydent naruszenia ochrony danych osobowych, po uprzednim telefonicznym lub osobistym zgłoszeniu, sporządza informację, która zawiera:

- Imię i nazwisko osoby zgłaszającej,
- Nazwę komórki organizacyjnej,
- Miejsce i datę wystąpienia incydentu,
- Opis incydentu oraz możliwe skutki,
- Podjęte działania zaradcze,

i przekazuje ją bezzwłocznie do IOD celem dalszego procedowania.

5.5. Administrator przy współudziale IOD dokonuje analizy ryzyka naruszenia praw i wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa, celem uniemożliwienia

wystąpienia podobnych zdarzeń w przyszłości.

5.6. W przypadku wystąpienia incydentu naruszenia ochrony danych osobowych, który skutkuje naruszeniem praw i wolności osób fizycznych, Administrator w terminie 72 godzin od stwierdzenia naruszenia, zgłasza je Prezesowi UODO, zgodnie z art. 33 RODO, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

5.7. Jeśli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, Administrator, zgodnie z art. 34 RODO zawiadamia również osobę , której dane dotyczą, o takim naruszeniu.

6. ODPOWIEDZIALNOŚĆ I KOMPETENCJE ADMINISTRATORA DANYCH OSOBOWYCH

6.1. Do obowiązków Administratora należy:

1) zapewnienie środków technicznych i organizacyjnych do ochrony przetwarzanych danych osobowych, odpowiednio do zagrożeń oraz kategorii danych objętych ochroną, w szczególności danych przed:
   - udostępnieniem osobom nieupoważnionym,
   - wykorzystaniem przez osobę nieuprawnioną,
   - zmianą, utratą, uszkodzeniem lub zniszczeniem;
2) zapewnienie legalności zabezpieczeniem przetwarzania danych osobowych, a w szczególności 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 oraz normami społecznymi,
   - dane zbierane były w oznaczonym, zgodnym z prawem celem,
   - dane były merytorycznie poprawne a ich zakres adekwatny do celu przetwarzania,
   - dane były przetwarzane w uzasadnionym, dostosowanym do celu, ograniczonym okresie czasu;
3) wyznaczenie Inspektora Ochrony Danych (ewentualnie Zastępcy Inspektora Ochrony Danych, który będzie realizować zadania IOD podczas jego nieobecności);
4) wydawanie imiennych upoważnień do przetwarzania danych osobowych i zarządzanie nimi;
5) dopuszczanie do przetwarzania danych osobowych wyłącznie osób przeszkolonych w

zakresie ochrony danych osobowych;

6) nadzorowanie zgodnego z prawem udostępniania i powierzania danych osobowych;
7) zgłoszenie do organu nadzorczego naruszenia ochrony danych osobowych bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, chyba że AD jest w stanie wykazać zgodnie z zasadą rozliczalności, że jest mało prawdopodobne, by naruszenie to mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych;
8) zapewnienie osobom, których dane dotyczą uzyskania informacji o:
   - celu, zakresie i sposobie przetwarzania danych,
   - terminie przetwarzania danych,
   - źródle, z którego dane pochodzą,
   - sposobie udostępniania danych oraz ich odbiorcach.

6.2. Do obowiązków Administratora w stosunku do IOD należy:

1) właściwie i niezwłoczne włączenie we wszystkie sprawy dotyczące ochrony danych osobowych,
2) wspieranie w wypełnianiu zadań, zapewniając mu zasoby niezbędne do wykonywania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej,
3) gwarantowanie działania bez presji i otrzymywania instrukcji dotyczących wykonywania zadań,
4) publikacja danych kontaktowych IOD oraz zawiadomienie o nich organu nadzorczego.

6.3. Administrator prowadzi RCPD oraz RKCPD.

6.4. Administrator nadzoruje działania IOD oraz wydaje mu zalecenia, co do sposobu wykonywania obowiązków wynikających z PBDO.

7. ZADANIA INSPEKTORA OCHRONY DANYCH

7.1. Do zadań IOD należy:

1) informowanie Administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie,
2) monitorowanie przestrzegania RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk AD lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia osób uczestniczących w operacjach przetwarzania oraz powiązane z tym

audyty,

3) przygotowanie oraz nadzór nad imiennymi upoważnieniami do przetwarzania danych osobowych (w tym coroczna weryfikacja aktualności podstaw prawnych wydanych upoważnień),
4) opiniowanie umów, które zawierają postanowienia dotyczące przetwarzania danych osobowych,
5) wspomaganie AD w tworzeniu i prowadzeniu RCPD, zgodnie z art. 30 ust. 1 RODO, którego wzór stanowi załącznik nr 4 do PBDO,
6) wspomagania AD w tworzeniu i prowadzeniu RKCPD, zgodnie z art. 30 ust. 2 RODO, którego wzór stanowi załącznik nr 6 do PBDO,
7) prowadzenie ewidencji incydentów z zakresu naruszenia bezpieczeństwa zasad ochrony danych osobowych,
8) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO, ocena skutków dla ochrony danych,
9) współpraca z organem nadzorczym,
10) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO uprzednie konsultacje, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach,
11) pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą w sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy art. 15-22 RODO,
12) weryfikacja zgodności przetwarzania danych osobowych z przepisami RODO oraz opracowanie w tym zakresie raz na rok sprawozdania dla Administratora,

7.2. IOD wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

7.3. Dane kontaktowe IOD (imię, nazwisko, adres e-mail):

1) są publikowane na stronie internetowej AD,
2) są zgłaszane Prezesowi UODO w sposób opisany w art. 10 USTAWY.

8. ZADANIA ADMINISTRATORA BEZPIECZEŃSTWA SYSTEMÓW

8.1. Do zadań ABS należy:

1) przestrzeganie zasad ochrony danych osobowych określonych w Polityce bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych

osobowych i dokumentach z nimi związanych,

2) zapewnienie prawidłowej eksploatacji systemu informatycznego w zakresie przetwarzania danych osobowych,
3) nadzorowanie wykonywania kopii zapasowych, odpowiedniego ich przechowywania oraz okresowego sprawdzania pod kątem ich dalszej przydatności do odtwarzania danych osobowych w przypadku awarii systemu,
4) zapewnienie ochrony nośników zawierających kopie zbiorów danych osobowych,
5) realizacja wytycznych AD w zakresie ochrony danych osobowych przetwarzanych z wykorzystaniem narzędzi informatycznych,
6) wyjaśnianie i usuwanie zgłoszonych nieprawidłowości lub incydentów związanych z przetwarzaniem danych osobowych w systemie informatycznym,
7) współpraca z IOD w zakresie bezpieczeństwa i zasad przetwarzania danych osobowych w systemach informatycznych.

9. ZADANIA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

9.1. Do przetwarzania danych u AD dopuszczone są jedynie osoby upoważnione przez AD.

9.2. Upoważnienie jest nadawane zgodnie ze wzorem stanowiącym załącznik nr 1 do PBDO.

9.3. Do zadań osób upoważnionych należy:

1) zapoznanie się z zasadami określonymi w PBDO oraz podpisanie oświadczenia o zapoznaniu się z tym dokumentem, którego wzór stanowi załącznik nr 7 do PBDO,
2) przestrzeganie zasad określonych w PBDO,
3) zachowanie w tajemnicy danych osobowych oraz informacji o sposobie ich zabezpieczenia,
4) ochrona danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem.

9.4. Działanie lub zaniechanie osoby upoważnionej, w wyniku którego doszło do naruszenia przestrzegania procedur lub poleceń może:

1) mieć konsekwencje dyscyplinarne,
2) zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych (w przypadku współpracy na podstawie Kodeksu pracy),
3) zostać uznane za ważny powód uzasadniający wypowiedzenie lub rozwiązanie umowy będącej podstawą współpracy.

9.5. Po zakończeniu współpracy z AD upoważnienie do przetwarzania danych osobowych automatycznie wygasa.

10. POSTANOWIENIA KOŃCOWE

10.1. Wszyscy pracownicy i inne osoby upoważnione do przetwarzania danych osobowych w Związku Powiatowo – Gminnym „Wielkopolski Transport Regionalny" z siedzibą w Poznaniu są zobowiązani do zapoznania się z treścią PBDO.

10.2. PBDO wchodzi w życie z dniem określonym w odpowiedniej uchwale AD.

10.3. Wszelkie zmiany Polityki bezpieczeństwa obowiązują od dnia ich wprowadzenia w sposób określony w ust. 10.2 powyżej.

10.4. Jakiekolwiek zmiany wprowadzane w załącznikach do niniejszej PBDO nie wymagają zmiany Polityki bezpieczeństwa.

10.5. Z dniem wprowadzenia Polityki bezpieczeństwa traci ważność wcześniej obowiązująca u AD dokumentacja ochrony danych osobowych.

10.6. W sprawach nieuregulowanych w niniejszej Polityce bezpieczeństwa mają zastosowanie przepisy powszechnie obowiązującego prawa, w tym przepisy o ochronie danych osobowych.

11. STRUKTURA DOKUMENTU POLITYKI BEZPIECZEŃSTWA DANYCH OSOBOWYCH

11.1. Polityka bezpieczeństwa składa się z niniejszego dokumentu PBDO oraz Załączników:

- Wzór upoważnienia do przetwarzania danych osobowych - załącznik nr 1
- Wzór oświadczenia firmy zewnętrznej o zachowaniu poufności informacji chronionych - załącznik nr 2
- Schemat udostępniania danych - załącznik nr 3
- Wzór rejestru czynności przetwarzania danych RCPD - załącznik nr 4
- Wzór zgłoszenia zbioru danych - załącznik nr 5
- Wzór rejestru kategorii czynności przetwarzania danych RKCPD - załącznik nr 6
- Oświadczenie o zapoznaniu się z Polityką bezpieczeństwa - załącznik nr 7

PRZEWODNICZĄCY ZARZĄDU
ZWIĄZKU
Piotr Hojan

Poznań, dnia .....

UPOWAŻNIENIE nr ..... /rok

Na podstawie art. 29 Rozporządzenia 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 chronię danych) oraz Polityki Bezpieczeństwa Ochrony Danych Osobowych w Związku Powiatowo-Gminnym „Wielkopolski Transport Regionalny" w Poznaniu (**Administrator**), **upoważniam Pana/Panią**

imię + nazwisko
stanowisko

w celu realizacji zadań powierzonych na zajmowanym stanowisku:

1) do przetwarzania danych osobowych (w szczególności ich zbierania, utrwalania, organizowania, porządkowania, przechowywania, adaptowania lub modyfikowania, pobierania, przeglądania, wykorzystywania, ujawniania poprzez przesłanie, rozpowszechniania lub innego rodzaju udostępniania, dopasowywania lub łączenia, ograniczania, usuwania lub niszczenia) w formie papierowej jak i elektronicznej wyłącznie w zakresie wynikającym z zadań służbowych oraz poleceń służbowych przełożonego w następujących zbiorach:
   a) ..... (numer i nazwa zbioru)
   b) ..... (numer i nazwa zbioru)

2) do przetwarzania danych osobowych zawartych w systemie/aplikacji (nazwa + rodzaj uprawnień).

Pan/Pani imię + nazwisko został przeszkolony w dniu .....w zakresie ochrony danych osobowych i zapoznał/a się z „Polityką Bezpieczeństwa Ochrony Danych Osobowych".

Upoważnienie zostaje udzielone na okres od dnia .....2024 r. do odwołania lub zakończenia świadczenia pracy bądź usług na rzecz Administratora.

Jednocześnie nakładam obowiązek zabezpieczania danych osobowych przed ich udostępnieniem osobom nieuprawnionym, zabraniem, zniszczeniem lub uszkodzeniem a także do zachowania ich w tajemnicy.

Obowiązek ten istnieje również po zakończeniu pracy na stanowisku.....
Traci ważność upoważnienie z dnia ..... znak .....

Data i podpis Administratora[1]

[1] Osoba uprawniona do reprezentowania Administratora.

Niniejszym potwierdzam zapoznanie się z treścią obowiązujących u Administratora regulacji dotyczących ochrony danych osobowych i bezpieczeństwa informacji, w szczególności Polityki Bezpieczeństwa Ochrony Danych Osobowych i zobowiązuję się do ich przestrzegania. Zobowiązuję się zachować w tajemnicy dane osobowe, do których będę mieć dostęp oraz sposoby ich zabezpieczenia, także po wygaśnięciu niniejszego upoważnienia. Przyjmuję do wiadomości, że udostępnienie danych osobowych lub umożliwienie dostępu do tych danych osobom nieupoważnionym może podlegać odpowiedzialności, szczególnie odpowiedzialności karnej, zgodnie z powszechnie obowiązującymi przepisami.

Data i podpis osoby upoważnionej[2]

PRZEWODNICZĄCY ZARZĄDU
ZWIĄZKU
Piotr Mojan

[2] Osoba współpracująca z Administratorem (niezależnie od stażu pracy, zajmowanego stanowiska lub podstawy współpracy).

Poznań, dnia .....

Nazwa firmy, imię i nazwisko

adres

Oświadczenie firmy zewnętrznej o zachowaniu poufności informacji chronionych

1. Za „Informacje chronione" w rozumieniu niniejszego oświadczenia uważa się wszelkie zagadnienia techniczne, finansowe lub handlowe, w szczególności dane osobowe w rozumieniu Rozporządzenia 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, oraz inne dane prawnie chronione przez Związek Powiatowo-Gminny „Wielkopolski Transport Regionalny" w Poznaniu. Ponadto za „informacje chronione" mogą być również uważane dane powiązane z czynnościami wykonywanymi w Związku Powiatowo-Gminnym „Wielkopolski Transport Regionalny" w Poznaniu lub mające na nie wpływ.
2. Zobowiązuję się do zachowania w poufności Informacji chronionych w Związku Powiatowo-Gminnym „Wielkopolski Transport Regionalny" w Poznaniu. Jednocześnie zobowiązuję się do zachowania poufności sposobów zabezpieczenia informacji chronionych Związku Powiatowo-Gminnym „Wielkopolski Transport Regionalny" w Poznaniu również po zakończeniu wykonywania obowiązków lub innych zadań dla Związku Powiatowo-Gminnym „Wielkopolski Transport Regionalny" w Poznaniu.
3. Niniejsze oświadczenie obliguje mnie do przestrzegania warunków zawartych w umowie łączącej mnie ze Związkiem Powiatowo-Gminnym „Wielkopolski Transport Regionalny" w Poznaniu we wskazanym zakresie danych i informacji przetwarzanych na stanowisku pracy. Zobowiązuję się nie wykorzystywać żadnych danych oraz informacji bez upoważnienia w celu innym niż wykonywanie wyżej wymienionej umowy.
4. Oświadczam, że znana jest mi odpowiedzialność za naruszenie przepisów RODO, co w szczególności może stanowić podstawę do podjęcia przez Związek Powiatowo-Gminny „Wielkopolski Transport Regionalny" w Poznaniu przysługujących mu środków prawnych.

.....

Data i podpis osoby upoważnionej[1]

.....

Inspektor Ochrony Danych

PRZEWODNICZĄCY ZARZĄDU ZWIĄZKU

Piotr Hojan

[1] Osoba uprawniona do reprezentowania firmy zewnętrznej.

Schemat udostępniania danych:

1.1. Wpłynięcie żądania udostępnienia danych.

1.2. Potwierdzenie tożsamości wnioskodawcy - w razie braku możliwości potwierdzenia tożsamości, udzielenie odpowiedzi o braku możliwości rozpoznania żądania, z podaniem i wyjaśnieniem powodu.

1.3. Ustalenie opłaty/decyzja co do odmowy - weryfikacja, czy wniosek jest nadmierny lub ewidentnie nieuzasadniony, lub czy jest to wniosek o kolejną kopię danych.

1.4. Ustalenie, czy dane wnioskodawcy są przetwarzane - w razie niezidentyfikowania przetwarzania danych wnioskodawcy odpowiedź, że nie przetwarzamy danych wnioskodawcy.

1.5. Merytoryczna analiza żądania pod kątem jego zasadności i precyzji żądań.

1.6. Prośba o uściślenie, jeśli jest taka potrzeba.

1.7. Rozpoznanie żądania wnioskodawcy - w przypadku opóźnienia w rozpoznaniu żądania przekazanie wnioskodawcy informacji o przedłużeniu terminu, ze wskazaniem przyczyn opóźnienia oraz planowanego terminu udzielania odpowiedzi; w przypadku bezczynności Administratora danych osobowych, poinformowanie wnioskodawcy o przyczynach niepodjęcia działań oraz jego uprawnieniach z tym związanych.

1.8. Spełnienie żądania i udzielenie merytorycznej odpowiedzi wnioskodawcy.

PRZEWODNICZĄCY ZARZĄDU
ZWIĄZKU
Piotr Hojan

	REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH (ART. 30 UST. 1 RODO)
AD	ZWIĄZEK POWIATOWO-GMINNY "WIELKOPOLSKI TRANSPORT REGIONALNY" W POZNANIU

Lp.	Czynność przetwarzania	Cele przetwarzania	Kategorie osób, których dane dotyczą	Kategorie danych osobowych	Kategorie odbiorców [1]	Przekazanie danych do państwa trzeciego [2]	Planowane terminy usunięcia danych	Opis środków bezpieczeństwa [3]	Współadministratorzy
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									
13									
14									
15									
16									

[1] Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych.
[2] Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń.

[3] Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

PRZEWODNICZĄCY ZARZĄDU
ZWIĄZKU
Piotr Hojan

Zbiór danych osobowych

na stanowisku

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

Należy przez to rozumieć zestaw (rejestr, ewidencję, posegregowane dokumenty, spisy) zawierający dane osobowe, które można posortować, poukładać wg określonego klucza, może być zarówno papierowy jak i elektroniczny (Word, Excel, dowolna aplikacja biurowa)

1. Zgłoszenie nowego zbioru .....
2. Aktualizacja istniejącego zbioru .....
   1) **Nazwa Zbioru:**

      .....
   2) **Podstawa prawna upoważniająca do prowadzenia zbioru danych:**

      .....
   3) **Cel przetwarzania zbioru danych osobowych:**

      .....
   4) **Opis kategorii osób, których dane są przetwarzane:**

      .....
3. **Zakres danych przetwarzanych w zbiorze:**

□	Nazwisko i imię	□	miejsce pracy
□	Imiona rodziców	□	zawód
□	Data urodzenia	□	wykształcenie
□	Adres zamieszkania	□	seria i numer dowodu
□	Nr ewidencyjny PESEL	□	nr telefonu

4. **Inne dane osobowe nie wymienione w pkt 3 (np e-mail):**

   .....
5. **Zbiór zawiera dane wrażliwe TAK/NIE (***Jeżeli wybrano odpowiedź **TAK**, należy wskazać dane wrażliwe):*

- □ pochodzenie rasowe
- □ pochodzenie etniczne
- □ poglądy polityczne
- □ przekonania religijne
- □ przekonania filozoficzne
- □ przynależność wyznaniowa
- □ skazania
- □ orzeczenie o ukaraniu
- □ przynależność partyjna
- □ przynależność związkowa
- □ stan zdrowia
- □ kod genetyczny
- □ nałogi
- □ życie seksualne
- □ mandaty karne
- □ inne orzeczenia wydane w postępowaniu sądowym lub administracyjnym

6. **Podstawa prawna przetwarzania danych wrażliwych:**

.....

7. **Sposób zbierania danych zawartych w zbiorze:**
   - □ Wyłącznie od osób, których dotyczą
   - □ Głównie od osób, których dotyczy
   - □ Wyłącznie z innych źródeł
   - □ Głównie z innych źródeł
   - □ Głównie metodą teletransmisji
   - □ Również metodą teletransmisji
8. **Komu udostępniane będą dane ze zbioru:**
   - □ dane nie będą udostępniane innym podmiotom
   - □ dane będą udostępniane wyłącznie podmiotom na podstawie przepisów prawa
   - □ dane będą udostępniane innym podmiotom (*np. jeżeli na podstawie umowy, proszę wskazać nr umowy i czas na jaki została zawarta)*
   - □ dane będą udostępniane również drogą teletransmisji
   - □ dane będą udostępniane za granicę *(podaj nazwę kraju i na jakiej podstawie są przekazywane)*
9. **Odbiorcy danych lub ich kategorie** *(odbiorcą danych jest każdy komu udostępniamy dane):*

.....

10. **Czy dane są lub będą przekazywane do państwa trzeciego (spoza Unii Europejskiej)** *(podaj nazwę kraju i na jakiej podstawie są przekazywane)*

.....

11. **Okres przetwarzania - planowany termin usunięcia danych**: .....
12. **Od kiedy prowadzony jest zbiór** (*data jeżeli jest to możliwe):* .....
13. **Sposób przetwarzania:**
    - □ papierowy
    - □ elektronicznie - aplikacja biurowa (podaj nazwę aplikacji WORD, EXCEL itp.)

□ elektronicznie w systemie, aplikacji (podaj nazwę)

14. **Listę pracowników uprawnionych do przetwarzania danych w zgłaszanym zbiorze** *(imię, nazwisko, stanowisko).*

Podpis osoby odpowiedzialnej za prowadzony zbiór

PRZEWODNICZĄCY ZARZĄDU
ZWIĄZKU
Piotr Hojan

REJESTR KATEGORII CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH (ART. 30 UST. 2 RODO)	
Podmiot przetwarzający	ZWIĄZEK POWIATOWO-GMINNY "WIELKOPOLSKI TRANSPORT REGIONALNY" W POZNANIU

Lp.	Dane administratora [1]	Kategorie przetwarzań	Przekazanie danych do państwa trzeciego [2]	Opis środków bezpieczeństwa [3]
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				

[1] Imię i nazwisko lub nazwa oraz dane kontaktowe każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych.

[2] Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń.

PRZEWODNICZĄCY ZARZĄDU
ZWIĄZKU

Piotr Hojan

OŚWIADCZENIE PRACOWNIKA O ZAPOZNANIU SIĘ Z POLITYKĄ BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH

Ja, niżej podpisany/a *imię i nazwisko,* zamieszkały/a w *adres,*
zatrudniony/a w Związku Powiatowo-Gminnym „Wielkopolski Transport Regionalny" w Poznaniu
na stanowisku: *stanowisko,*
oświadczam, że:

1) zapoznałem/am się z Polityką Bezpieczeństwa Ochrony Danych Osobowych,
2) zobowiązuje się do przestrzegania Polityki Bezpieczeństwa Ochrony Danych Osobowych.

Data i podpis pracownika

Data i podpis osoby przyjmujące oświadczenie

PRZEWODNICZĄCY ZARZĄDU
ZWIĄZKU
Piotr Hojan