

POLITYKA BEZPIECZEŃSTWA
PRZETWARZANIA DANYCH OSOBOWYCH
ORAZ
INSTRUKCJA BEZPIECZEŃSTWA
SYSTEMÓW INFORMATYCZNYCH
w Zarządzie Drogowym
w Sępólnie Krajeńskim



Sępólno Krajeńskie, 25 maja 2018 r.

Rozdział 1 Postanowienia ogólne

§ 1.

„Polityka Bezpieczeństwa przetwarzania danych osobowych oraz instrukcja bezpieczeństwa systemów informatycznych”, zwana dalej „Polityką”, została opracowana na podstawie wytycznych zawartych w rozporządzeniu Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 roku 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.

„Polityka” określa podstawowe zasady przetwarzania danych osobowych w Zarządzie Drogowym w Sępólnie Krajeńskim oraz środki techniczne i organizacyjne zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych w systemach tradycyjnych oraz systemach informatycznych, zgodnie z rozporządzeniem.

§ 3.

Ilekróć w „Polityce” jest mowa o:

1. **RODO** – rozumie się przez to rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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. **Administratorze danych osobowych** – rozumie się przez to Dyrektora Zarządu Drogowego w Sępólnie Krajeńskim.
3. **Inspektorze Ochrony Danych (IOD)** – należy przez to rozumieć osobę wyznaczoną przez Administratora danych osobowych do pełnienia funkcji, o której mowa w art. 37 RODO, która jest odpowiedzialna za zapewnienie przestrzegania przepisów o ochronie danych osobowych w Zarządzie Drogowym w Sępólnie Krajeńskim.
4. **Użytkownik** – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w ramach wykonywanych zadań.
5. **Danych osobowych** – należy przez to rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. 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 IP, lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
6. **Zbiór danych** – należy przez to rozumieć uporządkowany zestaw danych osobowych dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
7. **Przetwarzaniu danych** – należy przez to rozumieć operacje wykonywane na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczenie, usuwanie lub niszczenie.
8. **Systemie informatycznym** – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych.
9. **Podmiocie przetwarzającym** – należy przez to rozumieć osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora danych osobowych.
10. **Profilowaniu** – należy przez to rozumieć dowolną formę 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, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania itp.

11. **Pseudonimizacji** – należy przez to rozumieć przetwarzanie danych osobowych w taki sposób, aby nie można było już ich przypisać konkretnej osobie bez użycia dodatkowych informacji.
12. **Anonimizacji** – należy przez to rozumieć uniemożliwienie wszystkim stronom zidentyfikowania konkretnej osoby.

Rozdział 2

Polityka Bezpieczeństwa przetwarzania danych osobowych

§ 4.

Zakres stosowania

1. W Zarządzie Drogowym w Sępólnie Krajeńskim przetwarzane są w szczególności dane osobowe petentów i pracowników, które zbierane są w zbiory danych.
2. Informacje te są przetwarzane zarówno w systemie tradycyjnym, jak i informatycznym.
3. Do informacji przechowywanych w systemach mają dostęp jedynie upoważnieni pracownicy Zarządu Drogowego oraz inne upoważnione osoby zajmujące się obsługą systemów oraz osoby kontrolujące jednostkę. Wszyscy zobowiązani są do zachowania danych w tajemnicy.

§ 5.

Obszar przetwarzania danych osobowych

1. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe określa załącznik nr 1 do „Polityki”.
2. Przetwarzanie danych osobowych z użyciem stacjonarnego sprzętu komputerowego i kartotek odbywa się wyłącznie w obszarze przetwarzania danych.
3. Stały dostęp do pomieszczeń, w których przetwarzane są dane osobowe, mają tylko ich użytkownicy.
4. Dostęp do pomieszczeń, w których przetwarzane są dane osobowe, osób innych niż osoby pracujące na tych zbiorach, jest możliwy wyłącznie w obecności co najmniej jednego użytkownika za zgodą Administratora danych osobowych.
5. Kartoteki, zbiory danych, elektroniczne nośniki informacji należy przechowywać w przeznaczonych do tego szafach biurowych, do których dostęp mają wyłącznie użytkownicy. Po godzinach pracy szafy zamykane są na klucz.
6. Proces przetwarzania danych osobowych w godzinach pracy odbywa się pod kontrolą upoważnionych pracowników. Po godzinach pracy pomieszczenia służbowe zostają zabezpieczone fizycznie, a cały obiekt jest chroniony systemem alarmowym.
7. W przypadku wystąpienia incydentu w Zarządzie Drogowym w Sępólnie Krajeńskim Administrator Danych osobowych lub inna wybrana osoba, powiadamia niezwłocznie o tym fakcie Inspektora Ochrony Danych.

§ 6.

Rejestr czynności przetwarzania danych osobowych

1. Czynności przetwarzania danych, to zespół powiązanych ze sobą operacji na danych osobowych, wykonywanych przez jedną lub kilka osób, które można określić w sposób zbiorczy, w związku z celem, w jakim te czynności są podejmowane.
2. Rejestr czynności przetwarzania danych osobowych stanowi załącznik nr 2 do niniejszej „Polityki”.
3. W sytuacji, gdy Zarząd Drogowy w Sępólnie Krajeńskim będzie przetwarzał dane osobowe, jako podmiot przetwarzający (nastąpi powierzenie danych osobowych), zobowiązany będzie do prowadzenia rejestru kategorii czynności przetwarzania, według wzoru określonego załącznikiem nr 3 do „Polityki”.
4. Rejestry prowadzi IOD w formie papierowej lub elektronicznej, w których inwentaryzuje i monitoruje sposób, w jaki Zarząd Drogowy wykorzystuje dane osobowe.

§ 7.

Zadania Inspektora Ochrony Danych

Do zadań IOD należy w szczególności:

1. Informowanie Administratora danych osobowych, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia oraz innych przepisów o ochronie danych osobowych oraz doradzanie im w tych sprawach.
2. Monitorowanie przestrzegania rozporządzenia, innych przepisów o ochronie danych osobowych oraz niniejszej „Polityki”.
3. Przeprowadzanie audytów, szkoleń oraz inicjowanie wszelkich innych działań podnoszących świadomość użytkowników przetwarzających dane osobowe.
4. Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych.
5. Prowadzenie rejestrów zbiorów oraz rejestrów czynności przetwarzania.
6. Współpraca z Urzędem Ochrony Danych Osobowych.
7. Pełnienie funkcji punktu kontaktowego dla Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 rozporządzenia, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.
8. Pełnienie punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy rozporządzenia i innych przepisów dotyczących ochrony danych osobowych.
9. Sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla Administratora danych osobowych.
10. Przygotowanie upoważnień do przetwarzania danych oraz umów w zakresie powierzenia danych osobowych.
11. Opracowanie i stała aktualizacja dokumentacji oraz instrukcji dotyczących bezpieczeństwa danych osobowych.

§ 8.

Wykaz zbiorów danych osobowych przetwarzanych w zbiorach papierowych oraz w systemie informatycznym.

1. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych określa załącznik nr 4 do „Polityki”.
2. Opis struktury zbiorów danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między poszczególnymi programami i systemami stosowanymi w Zarządzie Drogowym w Sepólnie Krajeńskim określa załącznik nr 5 do „Polityki”:

§ 9.

Środki techniczne i organizacyjne zabezpieczenia danych osobowych.

1. Administrator danych osobowych decyduje o celach i środkach przetwarzania danych osobowych i jest odpowiedzialny za całościowy proces wdrożenia odpowiednich środków technicznych i organizacyjnych, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania.
2. Użytkownik jest odpowiedzialny przed Administratorem danych osobowych za nadzór i utrzymanie niezbędnych warunków bezpieczeństwa, w szczególności do przestrzegania procedur dostępu i ochrony danych osobowych.
3. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie wydane przez Administratora danych osobowych. Wzór upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 6 do „Polityki”.
4. Inspektor Ochrony Danych prowadzi rejestr wydanych upoważnień, w którym odnotowuje również datę ustania takiego upoważnienia. Rejestr prowadzony jest według wzoru określonego w załączniku nr 7 do niniejszej „Polityki”.
5. Upoważnienie wygasa w przypadku:
 - a) ustania stosunku pracy;
 - b) zakończenia wykonywania prac określonych umową cywilnoprawną (np. umową zlecenia);
 - c) zakończenia kontraktu z kontrahentem zewnętrznym;
 - d) zmianą stanowiska służbowego;
 - e) zaistnienia sytuacji (zgodnie z zasadą „wiedzy koniecznej”). Gdy pracownik nie potrzebuje już dostępu do konkretnego zbioru danych, aby świadczyć stosunek pracy.

6. Każdy pracownik przed rozpoczęciem pracy, z którą wiąże się przetwarzanie danych osobowych, musi zostać przeszkolony przez Inspektora Ochrony Danych w zakresie obowiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz informacji o zagrożeniach związanych z przetwarzaniem danych osobowych w systemie informatycznym i tradycyjnym. Po odbyciu szkolenia pracownik podpisuje oświadczenie o zapoznaniu się z przepisami o ochronie danych osobowych według wzoru określonego w załączniku nr 8 do „Polityki”.
7. Przed rozpoczęciem pracy na dokumentach w formie papierowej zawierających dane osobowe, przetwarzająca je osoba ma obowiązek upewnić się czy były próby nieuprawnionego dostępu do danych osobowych zawartych w dokumentach.
8. W przypadku ujawnienia, utraty lub podejrzenia ujawnienia bądź utraty danych osobowych, użytkownik niezwłocznie powiadamia Inspektora Ochrony Danych.
9. W przypadku krótkotrwałego opuszczenia miejsca pracy użytkownik jest zobowiązany do ich zabezpieczenia przed dostępem osób nieuprawnionych.
10. Po zakończeniu pracy dokumenty zawierające dane osobowe, należy zabezpieczyć przed dostępem osób nieuprawnionych w miejscach do tego przeznaczonych zamykanych na klucz.
11. Wydruki robocze, błędne lub zdezaktualizowane winny być niezwłocznie niszczone przy użyciu niszczarki.
12. Ewidencja, obieg i archiwizacja dokumentów zawierających dane osobowe odbywa się zgodnie z obowiązującą w Zarządzie Drogowym „Instrukcją kancelaryjną”.
13. Klucze do pomieszczeń przechowywane są w wyznaczonym miejscu (pok. nr 1 budynku głównego) w wiszącej na ścianie, metalowej skrzynce zamykanej na klucz i zabezpieczone po godzinach pracy przed ich nieuprawnionym użyciem.
14. Klucze zapasowe do pomieszczeń przechowywane są w sejfie. Wydanie upoważnionym pracownikom kluczy zapasowych może odbywać się tylko w uzasadnionych sytuacjach oraz przypadkach awaryjnych za zgodą Administratora danych osobowych.
15. Zabezpieczenie przed nieautoryzowanym dostępem:
 - a) identyfikacja użytkownika w systemie następuje poprzez zastosowanie indywidualnego loginu i hasła dostępu. System informatyczny zabezpieczony jest programem antywirusowym z zaporą antywłamaniową.
 - b) monitory ekranowe muszą być usytuowane w sposób uniemożliwiający odczyt danych przez osoby postronne, ponadto muszą posiadać wygaszacz ekranu.
 - c) nośniki danych zawierające kopie bezpieczeństwa przechowywane są w miejscach o ograniczonym i kontrolowanym dostępie.

§ 10.

Obowiązek informacyjny Administratora danych

1. Zgodnie z art. 13 ust. 1 RODO, jeżeli dane osobowe zbierane są od osoby, której dane dotyczą, Administrator zobowiązany jest podać jej następujące informacje:
 - a) swoją tożsamość i dane kontaktowe;
 - b) dane kontaktowe Inspektora Ochrony Danych;
 - c) cele przetwarzania danych, oraz podstawę prawną;
 - d) jeżeli dane osobowe są przetwarzane zgodnie z prawem (art. 6 ust. 1 lit.f) – prawnie uzasadniony interes realizowany przez administratora;
 - e) informacje o odbiorcach;
2. Ponadto, podczas pozyskiwania danych, administrator podaje osobie, której dane dotyczą, następujące informacje:
 - a) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe kryteria ustalenia tego okresu;
 - b) informacje o jego prawie do żądania do dostępu do tych danych;
 - c) prawie do cofnięcia zgody;
 - d) informacje o prawie wniesienia skargi;
 - e) informacje o profilowaniu itp.
3. Powyższy obowiązek w Zarządzie Drogowym w Sępólnie Krajeńskim winien być spełniony poprzez umieszczenie klauzuli informacyjnej na stronie internetowej oraz na tablicy ogłoszeń w jego siedzibie. Ponadto klauzula informacyjna musi być stosowana w korespondencji wychodzącej.

§ 11.

Powierzenie przetwarzania danych

1. Powierzenie przetwarzania danych osobowych występuje wówczas, gdy podmioty zewnętrzne współpracujące z Administratorem danych osobowych mają dostęp do danych osobowych przetwarzanych w Zarządzie Drogowym w Sępólnie Krajeńskim.
2. Powierzenie może mieć miejsce wyłącznie poprzez zawarcie stosownej pisemnej umowy powierzenia pomiędzy Administratorem danych osobowych, a podmiotem któremu powierzono przetwarzane dane osobowe.
3. Wzór umowy powierzenia stanowi załącznik nr 9 do „Polityki”.
4. IOD prowadzi rejestr podmiotów zewnętrznych, którym powierzono dane osobowe do przetwarzania według załącznika stanowiącego załącznik nr 10 do „Polityki”.

§ 12.

Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych.

1. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie systemu ochrony danych osobowych użytkownik zobowiązany jest do bezzwłocznego powiadomienia o tym fakcie Inspektora Ochrony Danych oraz Administratora danych osobowych.
2. Użytkownik do momentu przybycia Inspektora Ochrony Danych powinien:
 - a) zabezpieczyć dostęp do pomieszczenia i urządzeń;
 - b) powstrzymać się od rozpoczęcia lub kontynuowania jakichkolwiek czynności mogących spowodować zatarcie śladów, bądź dowodów naruszenia ochrony;
 - c) zatrzymać pracę na komputerze, na którym zaistniało naruszenie ochrony oraz nie uruchamiać innych urządzeń, które mogą mieć związek z naruszeniem ochrony;
 - d) podjąć, stosownie do zaistniałej sytuacji działania, które zapobiegą ewentualnej utracie danych osobowych.
 - e) nieopuszczanie bez uzasadnionej przyczyny miejsca zdarzenia do czasu przybycia IOD.
3. Inspektor Ochrony Danych po otrzymaniu informacji o naruszeniu lub próbie naruszenia zabezpieczenia systemu przetwarzającego dane osobowe, podejmuje działania zmierzające do usunięcia powstałego zagrożenia:
 - a) ocenia sytuację, uwzględniając stan pomieszczenia, w którym przetwarzane są dane, stan urządzenia i zbioru oraz identyfikuje zakres negatywnych następstw naruszenia ochrony danych osobowych;
 - b) wysłuchuje relacji użytkownika lub osoby, która dokonała powiadomienia;
 - c) podejmuje działania mające na celu ustalenie sprawcy, miejsca, czasu i sposobu dokonania naruszenia ochrony;
 - d) w zależności od zakresu naruszenia ochrony podejmuje decyzje o dalszym postępowaniu, wydając stosowne polecenia i wskazówki do obsługi urządzeń.
4. Inspektor Ochrony Danych dokumentuje zaistniały incydent sporządzając odpowiedni raport, który obejmuje:
 - a) dane osoby stwierdzającej naruszenie ochrony;
 - b) datę, godzinę i miejsce naruszenia ochrony;
 - c) rodzaj naruszenia ochrony oraz okoliczności temu towarzyszące
 - d) informacje o danych, które zostały lub mogły zostać ujawnione;
 - e) zabezpieczone materiały lub inne dowody związane z wydarzeniem;
 - f) opis podjętych czynnościRaport niezwłocznie po jego opracowaniu, przekazywany jest Administratorowi danych osobowych.
Wzór raportu o naruszeniu bezpieczeństwa danych osobowych stanowi załącznik nr 11 do „Polityki”.
5. W przypadku naruszenia ochrony danych osobowych Administrator danych osobowych wraz z Inspektorem Ochrony Danych bez zbędnej zwłoki, ale w terminie nie dłuższym niż 72 godziny po stwierdzeniu naruszenia zgłasza zaistniały incydent do Urzędu Ochrony Danych Osobowych według załącznika stanowiącego załącznik nr 12 do „Polityki”.
6. Administrator danych osobowych dokumentuje wszelkie zdarzenia związane z naruszeniem ochrony danych osobowych uwzględniając je w rejestrze naruszeń ochrony danych osobowych, stanowiącym załącznik nr 13 do „Polityki”.

§ 13.

Analiza ryzyka

1. Ryzykiem są wszelkie zdarzenia, które naruszają bezpieczeństwo danych osobowych.
2. W celu zapobieżenia naruszeniom danych osobowych należy przeprowadzić analizę ryzyka, która jest dokonywana na podstawie oceny ryzyka.
3. Do określenia akceptowalnego progu ryzyka w Zarządzie Drogowym w Sępólnie Krajeńskim stosuje się skalę trzystopniową: ryzyko małe, średnie i duże.

		prawdopodobieństwo incydentu		
		1	2	3
następstwa	1	1	2	3
	2	2	4	6
	3	3	6	9

1 - 2 – ryzyko **małe** (pomijalne i akceptowalne – nie podejmuje się żadnych działań)

3 - 4 – ryzyko **średnie** (akceptowalne - należy podjąć działania w celu minimalizacji ryzyka)

6 - 9 – ryzyko **duże** (nieakceptowane, należy podjąć środki zapobiegawcze, a jeżeli przyjęte rozwiązania nie minimalizują skutecznie ryzyka, należy skonsultować się z organem nadzoru)

4. Ocena ryzyka w Zarządzie Drogowym w Sępólnie Krajeńskim powinna być powtarzana i należy ją przeprowadzać nie rzadziej niż raz do roku lub każdorazowo w przypadku zmiany jakiegokolwiek elementu mającego wpływ na zmianę aktywów, zagrożeń, podatności, zabezpieczeń lub skutków.

Rozdział 3

Instrukcja bezpieczeństwa systemów informatycznych

§ 14.

Administrator Systemu Informatycznego

1. Dla zapewnienia bezpieczeństwa systemów informatycznych wyznacza się Administratora Systemu Informatycznego (ASI), który stanowi pomoc IOD w zakresie informatycznym w Zarządzie Drogowym w Sępólnie Krajeńskim.
2. Obowiązki ASI:
 - a) nadzoruje poprawność działania systemów informatycznych w Zarządzie Drogowym w Sępólnie Krajeńskim;
 - b) wdraża procedury bezpieczeństwa oraz prowadzi nadzór nad nimi;
 - c) wdraża procedury ochrony antywirusowej i nadzoruje profilaktykę antywirusową;
 - d) informuje Administratora danych osobowych oraz Inspektora Danych Osobowych o stwierdzonych naruszeniach bezpieczeństwa systemu teleinformatycznego oraz wykrytych wirusach;
 - e) zakłada konta i przydziela hasła użytkownikom, którzy przetwarzają dane osobowe;
 - f) doradza użytkownikom systemu komputerowego w zakresie bezpieczeństwa
 - g) uczestniczy w procesach szacowania ryzyka.

§ 15.

Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym

1. Rozpoczęcie pracy
 - a) Przetwarzanie danych osobowych w systemach informatycznych Zarządu Drogowego w Sępólnie Krajeńskim, może dokonywać wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych
 - b) przed rozpoczęciem pracy na komputerze użytkownik systemu ma obowiązek sprawdzić czy wyposażenie techniczne stanowiska jest kompletne i nie nosi śladów fizycznej ingerencji w narzędzia sprzętowe lub programowe przez osoby nieuprawnione;

- c) po włączeniu komputera należy ocenić jakość jego pracy i stwierdzić zmiany;
 - d) po uruchomieniu systemu należy zalogować się, wpisując swój identyfikator (login) i hasło dostępu nadane przez ASI;
 - e) należy zweryfikować stan programu antywirusowego, a w szczególności zwrócić uwagę czy jest uruchomiony i posiada aktualne bazy sygnatur wirusów.
 - f) ekran monitora należy ustawić tak, aby uniemożliwić podgląd osobom nieuprawnionym,
 - g) w przypadku krótkotrwałego opuszczenia stanowiska pracy, użytkownik systemu obowiązany jest uaktywnić wygaszacz ekranu zabezpieczony hasłem. Wygaszacz ekranu powinien być skonfigurowany tak, aby ekran komputera przetwarzającego dane osobowe był automatycznie blokowany po upływie 10 minut czasu nieaktywności użytkownika.
 - h) w razie konieczności dłuższego opuszczenia miejsca pracy użytkownik zobowiązany jest do wylogowania się z systemu i zabezpieczenia nośników elektronicznych i dokumentów zawierających dane osobowe;
 - i) należy stosować urządzenia zabezpieczające przed utratą danych, spowodowaną awarią zasilania lub zakłóceniem w sieci elektrycznej.
2. Zakończenie pracy
- a) po zakończeniu pracy użytkownik systemu zobowiązany jest prawidłowo wylogować się z systemu, wyłączyć komputer i zabezpieczyć stanowisko przed dostępem osób nieuprawnionych;
 - b) należy sprawdzić czy nie zostały pozostawione bez nadzoru nośniki informacji;
 - c) zaleca się po zakończeniu pracy stosowanie „polityki czystego biurka”;
 - d) przed wyjściem i zamknięciem pomieszczenie, w którym przetwarzane są dane osobowe, należy upewnić się, że szafy i biurka z dokumentacją są zamknięte.

§ 16.

Tworzenie kopii zapasowych i ich przechowywanie

1. W celu umożliwienia odtworzenia informacji zawartych w zbiorach danych osobowych tworzy się kopie zapasowe plików.
2. Kopie zapasowe plików tworzy się na dyskach zewnętrznym znajdujących się na wyposażeniu pracowników, których kopie zapasowe dotyczą.
3. Kopie zapasowe powinny być tworzone przynajmniej raz w miesiącu.
4. Nośniki informacji zawierające kopie zapasowe przechowywane są w miejscach zamykanych na klucz i chronione przed dostępem osób nieupoważnionych.
5. Za przechowywanie elektronicznych nośników informacji zawierających dane osobowe odpowiedzialny jest użytkownik tych nośników.
6. Bez zgody Administratora danych zabrania się wnoszenia elektronicznych nośników informacji zawierających dane osobowe. W przypadku uzyskania zgody dane zawarte na nośniku muszą być zaszyfrowane, by nikt nieupoważniony nie mógł go otworzyć.
7. Kopie zapasowe, które uległy uszkodzeniu lub stały się nieprzydatne, pozbawia się zapisu danych, a w przypadku, gdy nie jest to możliwe, niszczy się je w stopniu uniemożliwiającym ich odczytanie.
8. Czas przechowywania kopii zapasowych, jeżeli nie stanowią inaczej przepisy prawa, przechowuje się do momentu ich przydatności.

§ 17.

Oprogramowanie

1. Do instalowania sprzętu informatycznego oraz oprogramowania niezbędnego do pracy uprawniony jest wyłącznie wyznaczony pracownik zajmujący się obsługą informatyczną w Zarządzie Drogowym. Jest nim wyznaczony Administrator Systemów Informatycznych.
2. Na komputerach służbowych winny znajdować się wyłącznie oprogramowania niezbędne do wykonywania obowiązków pracowniczych i posiadające odpowiednią licencję na ich użytkowanie.
3. Zabrania się instalowania prywatnych programów, chyba że Administrator danych osobowych wyrazi na to zgodę, uważając że będzie to niezbędne do wykonywania zadań służbowych, nie zagraża bezpieczeństwu systemu, a użytkownik dysponuje licencją na oprogramowanie.
4. ASI ma prawo do kontrolowania legalności oprogramowania zainstalowanego na komputerach należących do Zarządu Drogowego w Sepólnie Krajeńskim.

5. Wszystkie komputery użytkowane w Zarządzie Drogowym w Sępólnie Krajeńskim muszą być chronione aktualnym oprogramowaniem antywirusowym z zaporą ogniową – Kaspersky Internet Security.

§ 18.

Sposoby zabezpieczenia systemu informatycznego przed działaniem złośliwego oprogramowania

1. Nośniki informacji z oprogramowaniem używanym w systemie informatycznym, jak również nośniki informacji zawierające dane osobowe, podlegają procedurze kontroli na obecność wirusów.
2. ASI odpowiedzialny jest za zainstalowanie programu antywirusowego i takie jego skonfigurowanie, aby uruchamiał się w trakcie startu systemu i pracował w tle skanując system w celu wykrycia ewentualnych wirusów.
3. Program antywirusowy uaktualnia się samoczynnie. ASI może wrywkowo zweryfikować czy aktualizacje wykonują się poprawnie.
4. Należy zachować szczególną ostrożność przy używaniu nośników pochodzących z zewnątrz każdorazowo sprawdzając je na obecność szkodliwego oprogramowania przed użyciem w systemie.
5. W przypadku stwierdzenia zawirusowania nośnika należy zgłosić to ASI. Zabrania się samowolnego usuwania wirusów przez użytkowników systemu.
6. ASI podejmuje działania mające na celu uniemożliwienie lub ograniczenie powstania szkód w wyniku działania wirusów oraz zabezpiecza zawirusowany nośnik w celu zidentyfikowania wyeliminowania zagrożenia.

§ 19.

Przeglądy i konserwacja systemów informatycznych

1. Przeglądy i konserwację systemów do przetwarzania danych osobowych wykonuje się w celu zapewnienia ciągłej i bezawaryjnej pracy tych systemów.
2. Zakres i częstotliwość wykonywania przeglądów oraz konserwacji systemów do przetwarzania danych osobowych określa instrukcja obsługi zainstalowanego sprzętu. W przypadku braku takich regulacji zakres i częstotliwość obsługi wyznacza ASI.
3. Wszelkie prace konserwacyjne i naprawcze w miejscu zainstalowania sprzętu mogą być wykonywane jedynie przez ASI lub pod jego nadzorem.
4. Prace dotyczące przeglądów, konserwacji i napraw wymagające zaangażowania autoryzowanych firm zewnętrznych, są wykonywane przez uprawnionych przedstawicieli tych firm.
5. Urządzenia komputerowe, dyski twarde lub inne informatyczne nośniki danych, przeznaczone do naprawy, pozbawia się najpierw zapisu danych osobowych.
6. Sprzęt do naprawy przekazuje ASI. Po odebraniu sprzętu z serwisu lub jego wymiany ASI dokonuje jego szczegółowych oględzin i instaluje go w systemie.
7. W przypadku awarii nośnika informacji (dysku twardego) ASI wycofuje go z eksploatacji i przechowuje, aż do chwili fizycznego zniszczenia.
8. Zużyte lub uszkodzone nośniki, o ile jest to technicznie możliwe muszą zostać poddane procedurze trwałego usunięcia danych przez użycie specjalistycznego oprogramowania narzędziowego do trwałego niszczenia danych lub fizycznie zniszczone w sposób uniemożliwiający odczyt danych z nośnika.
9. Zabrania się:
 - a) wnoszenia z pomieszczeń, gdzie zlokalizowano system przetwarzający dane osobowe wszelkich elementów wchodzących w jego skład;
 - b) samowolnej wymiany przez użytkownika jakiegokolwiek elementu składowego systemu;
 - c) pozostawienia nośnika informacji bez nadzoru;
 - d) przekazywania innemu podmiotowi nośników zawierających dane systemu, dokumenty użytkowników oraz baz danych, chyba że jest to podmiot uprawniony.
10. Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych. W tym celu stosuje się hasła dostępu do komputera przenośnego oraz do plików, w których przetwarzane są dane osobowe.

Rozdział 4
Postanowienia końcowe

1. Do zapoznania się z niniejszym dokumentem oraz stosowania zawartych w nim zasad zobowiązani są wszyscy pracownicy przetwarzający dane osobowe w Zarządzie Drogowym w Sępólnie Krajeńskim.
2. Użytkownik nieprzestrzegający zasad określonych w niniejszej Polityce ponosi odpowiedzialność dyscyplinarną.

Sporządził:

INSPEKTOR


Anita Kobus

Zatwierdził:

DYREKTOR
ZARZĄDU DROGOWEGO


inā. Edwini Eckert

ZARZĄD DROGOWY
w Sępólnie Kraj.
Powiat Sępoleński
ul. Korcnowska 5
89-400 Sępólno Krajeńskie
tel. (052) 388 12 02
NIP 561-133-56-37 Regon 092363449

Sępólno Krajeńskie, 25 maja 2018 roku

**Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar,
w którym przetwarzane są dane osobowe.**

1.	Wykaz pomieszczeń, w których przetwarzane są dane osobowe (wskazanie konkretnych nr lub oznaczeń pomieszczeń)	Numery pomieszczeń lub ich oznaczenia:
2.	Wykaz pomieszczeń, w których znajdują się komputery stanowiące element systemu informatycznego	Numery pomieszczeń lub ich oznaczenia:
3.	Wykaz pomieszczeń, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające komputerowe nośniki informacji z kopiami zapasowymi danych, stacje komputerowe, serwery i inne urządzenia komputerowe)	Numery pomieszczeń lub ich oznaczenia:
4.	Wykaz pomieszczeń, w których składowane są uszkodzone komputerowe nośniki danych (dyski, płyty, CD, dyski przenośne, uszkodzone komputery)	Numery pomieszczeń lub ich oznaczenia:
5.	Wykaz pomieszczeń archiwum	Numery pomieszczeń lub ich oznaczenia:
6.	Wykaz programów, w których przetwarzane są dane osobowe	np. Home Banking, Płatnik, program kadrowo – płacowy, MS Office
7.	Wykaz podmiotów zewnętrznych, które mają dostęp do danych osobowych lub je przetwarzają na podstawie podpisanych umów	

D Y R E K T O R
ZARZĄDU DRUGOWEGO

INA EDWINA ECKERT

ZARZĄD DRUGOWY
w Sępólnie Kraj.
Powiat Sępoleński
ul. Korcowska 5
89-400 Sępólno Krajeńskie
tel. (052) 388 17 02
NIP 561-133-56-37 Regon 692563499

Rejestr czynności przetwarzania danych osobowych

I.p.	Nazwa czynności przetwarzania	Cel przetwarzania	Kategorie osób	Kategorie danych osobowych	Planowany termin usunięcia kategorii danych	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa
1.						
2.						
3.						
...						

DYREKTOR
ZARZĄDU DROGOWEGO
inż. Robert Góral

ZARZĄD DROGOWY
w Sępólnie Kraj.
Powiat Sępoleński
ul. Korcnowska 5
89-400 Sępólno Krajeńskie
tel. (052) 388 12 02
NIP 561-133-56-35 Regon 0942344

Rejestr kategorii czynności przetwarzania

l.p.	Kategorie przetwarzania	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe)	Nazwa i dane kontaktowe Administratora	Inspektor Ochrony Danych	Czas trwania przetwarzania
1.					
2.					
3.					
...					

~~DYREKTOR~~
~~ZARZĄD DROGOWY~~
 -
 INŻ. EDWIN ŁECHOWI

ZARZĄD DROGOWY
 w Sępólnie Kraj.
 Powiat Sępoleński
 ul. Korcnowska 5
 89-400 Sępólno Krajeńskie
 tel. (052) 388 12 02
 NIP 561-133-56-37 Regon 092563442

**Wykaz zbiorów danych osobowych
wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych**

l.p.	Nazwa zbioru danych	Komórka organizacyjna przetwarzająca zbiór	Programy zastosowane do przetwarzania danych	Miejsce przetwarzania danych osobowych
1.				
2.				
3.				
...				

DYREKTOR
ZARZĄDU DRÓGOWEGO
inż. Ewelina Górska

ZARZĄD DRÓGOWY
w Sępólnie Kraj.
Powiat Sępoleński
ul. Korcnewska 5
89-400 Sępólno Krajeńskie
tel. (052) 388 17 02
NIP 561-133-56-37 Regon 09 030344

Upoważnienie do przetwarzania danych osobowych

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego 9UE_ 2016/679 z dnia 27 kwietnia 2016r. 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)

Upoważniam Panią / Pana

Stanowisko

do przetwarzania danych osobowych, których Administratorem jest
dyrektor Zarządu Drogowego w Sępólnie Krajeńskim
w zakresie pełnionych obowiązków służbowych na zajmowanym stanowisku

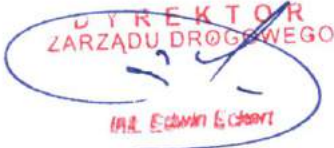
l.p.	Nazwa zbioru danych	Zakres uprawnień (dostęp, wprowadzenie, modyfikowanie, udostępnianie, usuwanie)
1.		
2.		
3.		
...		

Niniejsze upoważnienie obejmuje przetwarzanie danych osobowych w formie papierowej i / lub / w systemach informatycznych.

Okres ważności upoważnienia od do / na czas pełnienia obowiązków służbowych.

.....
Miejscowość i data nadania upoważnienia

.....
Administrator danych osobowych

**DYREKTOR
ZARZĄDU DROGOWEGO**

Marek Edzwini Edehart

**ZARZĄD DROGOWY
w Sępólnie Kraj.
Powiat Sępoleński
ul. Korcnowska 5
89-400 Sępólno Krajeńskie
tel. (052) 388 17 02
NIP 561-133-56-37 Regon: 092563469**

**Opis struktury danych osobowych wskazujący zawartość
poszczególnych pól informacyjnych i powiązania między nimi
oraz sposób przepływu danych pomiędzy poszczególnymi systemami**

l.p.	Nazwa zbioru danych	Struktura zbiorów	Przeływ danych
1.			
2.			
3.			
...			

DYREKTOR
ZARZĄDU DROGOWEGO
mgr Edwina Eckert

ZARZĄD DROGOWY
w Sępólnie Kraj.
Powiat Sępoleński
ul. Korcnowska 5
89-400 Sępólno Krajeńskie
tel. (052) 388 17 02
NIP 561-133-56-37 (Regon: 092563442)

Rejestr wydanych upoważnień

l.p.	Imię i nazwisko osoby upoważnionej	Stanowisko służbowe	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia (zbiory danych, nazwy systemów informatycznych)	Login / identyfikator (jeśli dane przetwarzane są w systemie informatycznym)
1.						
2.						
...						

DYREKTOR
ZARZĄDU DROGOWEGO

[Signature]

mgr. Ewelina Lichner

ZARZĄD DROGOWY
w Sępólnie Kraj.
Powiat Sępoleński
ul. Korcnowska 5
89-400 Sępólno Krajeńskie
tel. (052) 388 12 02
NIP 561-133-56-37 KRS 092363449

Oświadczenie o zapoznaniu się z przepisami o ochronie danych osobowych

Oświadczam, że zostałem/am zapoznany/a z przepisami dotyczącymi ochrony danych osobowych w **Zarządzie Drogowym w Sępólnie Krajeńskim, ul. Koronowska 5, 89-400 Sępólno Krajeńskie**, w szczególności wytycznymi Rozporządzenia Parlamentu Europejskiego i Rady UE 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) oraz wprowadzoną i wdrożoną do stosowania „Polityką bezpieczeństwa przetwarzania danych osobowych oraz Instrukcją bezpieczeństwa systemów informatycznych w Zarządzie Drogowym w Sępólnie Krajeńskim”

Jednocześnie zobowiązuję się do postępowania zgodnie z prawem oraz zachowania poufności danych osobowych, które przetwarza w trakcie wykonywania obowiązków służbowych. Zostałem/am poinformowany/a o odpowiedzialności związanej z przetwarzaniem danych osobowych.

.....
miejsowość i data

.....
czytelny podpis składającego oświadczenie

DYREKTOR
ZARZĄDU DROGOWEGO

inż. Edwin Eichert

ZARZĄD DROGOWY
w Sępólnie Kraj.
Powiat Sępoleński
ul. Koronowska 5
89-400 Sępólno Krajeńskie
tel. (052) 388 17 02
NIP 561-133-56-77 KRS 092363449

Umowa powierzenia przetwarzania danych osobowych

zawarta w dniu w

pomiędzy:

.....
.....
reprezentowanym przez dyrektora Zarządu Drogowego w Sepólnie Krajeńskim

zwanym dalej **Administratorem danych osobowych**

a

.....
.....
reprezentowanym przez

zwanym /ą dalej **Podmiotem przetwarzającym**

§ 1

Powierzenie przetwarzania danych osobowych

1. Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 r. dane osobowe zgodnie z obowiązującymi przepisami prawa, na zasadach i w celu określonym w niniejszej Umowie.
2. Podmiot przetwarzający oświadcza, że dysponuje środkami umożliwiającymi prawidłowe przetwarzanie danych osobowych powierzonych przez Administratora danych, w zakresie i celu określonym Umową.

§ 2

Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie umowy dane osobowe *(należy podać kategorię osób, których dane dotyczą) np. pracowników administratora, pracowników młodocianych, klientów administratora itd. w postaci np. imion i nazwisk, adresu zamieszkania, nr PESEL, nr telefonu, itd.*
2. Powierzone przez Administratora dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu *(należy podać cel przetwarzania danych przez podmiot przetwarzający np. realizacji umowy z dnia nr w zakresie prowadzenia kadr, realizacji umowy z dnia nr w zakresie obsługi finansowo-księgowej, itd.)*

§ 3

Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.
4. Podmiot przetwarzający, zgodnie z art. 28 ust. 3 pkt. b Rozporządzenia, zobowiązuje się zapewnić zachowanie w tajemnicy, przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
5. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem niezależnie od decyzji Administratora danych osobowych usuwa lub zwraca mu wszelkie dane

osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że szczególne przepisy prawa nakazują przechowywanie danych osobowych.

6. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.
7. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Administratorowi w ciągu 24 godzin od ujawnienia naruszenia.
8. Przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody Administratora danych.

§ 4

Prawo do kontroli

1. Administrator danych zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2. Administrator danych realizować będzie prawo do kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum 5 dniowym jego uprzedzeniem.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni
4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

§ 5

Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem, jeżeli nie dopełnił obowiązków, które nakłada niniejsza Umowa, lub gdy działał poza zgodnymi z prawem instrukcjami Administratora danych osobowych lub wbrew tym instrukcjom.

§ 6

Czas obowiązywania umowy

1. Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas *nieokreślony/określony* /*/ od do
2. Każda ze stron może wypowiedzieć niniejszą umowę z zachowaniem /*/ okresu wypowiedzenia.
3. Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym, gdy Podmiot przetwarzający:
 - a. pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
 - b. przetwarza dane osobowe w sposób niezgodny z umową;
 - c. powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych;

§ 7

Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
2. W zakresie nieuregulowanym niniejszą Umową zastosowanie mają przepisy Kodeksu cywilnego oraz Rozporządzenia.

.....
Administrator danych

ZARZĄD DRUGOWY
w Sępólnie Kraj.
Powiat Sępoleński
ul. Korcnowska 5
89-400 Sępólno Krajeńskie
tel. (052) 388 17 02
NIP 561-133-56-77 Regon 691353449

.....
Podmiot przetwarzający

DYREKTOR
ZARZĄDU DRUGOWEGO

Inż. Edwin Eckert

**Rejestr podmiotów zewnętrznych,
którym powierzono dane osobowe do przetwarzania**

l.p.	Nazwa firmy (podmiotu przetwarzającego)	Zakres świadczonych usług	Nr i data umowy	Uwagi (np. czas trwania umowy)
1.				
2.				
3.				
...				

~~DYREKTOR
ZARZĄDU DROGOWEGO~~
~~(M. Kucharski)~~

ZARZĄD DROGOWY
w Sępólnie Kraj.
Powiat Sępoleński
ul. Korcnowska 5
89-400 Sępólno Krajeńskie
tel. (052) 388 12 02
NIP 561-133-56-37 Regon 092361449

Raport o naruszeniu bezpieczeństwa danych osobowych

1. Data i godzina wystąpienia naruszenia
2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem (imię i nazwisko, stanowisko służbowe)
.....
.....
3. Lokalizacja zdarzenia (np. nr pomieszczenie, nazwa, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.)
.....
.....
4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności temu towarzyszące
.....
.....
5. Podjęte działania
.....
.....
6. Wstępna ocena przyczyn wystąpienia naruszenia
.....
.....
7. Postępowanie wyjaśniające i naprawcze
.....
.....
8. Zabezpieczone materiały lub inne dowody związane z wydarzeniem
.....
.....

.....
data

.....
podpis

DYREKTOR
ZARZĄDU DRÓGOWEGO

inż. Edwin Echert

ZARZĄD DRÓGOWY
w Sępólnie Kraj.
Powiat Sępoleński
ul. Korcnowska 5
89-400 Sępólno Krajeńskie
tel. (052) 388 17 02
NIP 561-133-56-37 Regon 14922374-9

Zgłoszenie naruszenia danych osobowych

1. Opis charakteru naruszenia ochrony danych osobowych, jaka kategoria, przybliżona liczba osób, których ten incydent dotyczy
.....
.....
2. Imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych oraz adres i oznaczenie punktu kontaktowego, od którego można uzyskać więcej informacji
.....
.....
3. Opis możliwych konsekwencji związanych z naruszeniem danych osobowych
.....
.....
4. Opis środków zastosowanych przed incydem i po wykryciu przypadku naruszenia ochrony danych osobowych
.....
.....

.....
podpis Administratora danych osobowych

DYREKTOR
ZARZĄDU DRÓGOWEGO
[Signature]
mgr EDYTA KUJAWA
ZARZĄD DRÓGOWY
w Sępólnie Kraj.
Powiat Sępoleński
ul. Korcnowska 5
89-400 Sępólno Krajeńskie
tel. (052) 388 12 02
NIP 561-153-56-37 Regon 142303141

Uwaga:

W przypadku naruszenia ochrony danych osobowych, Administrator danych osobowych, zgłasza ten przypadek do Urzędu Danych Osobowych, nie później niż w terminie 72 godzin po stwierdzeniu takiego naruszenia.

Rejestr naruszeń ochrony danych osobowych

Rodzaj naruszenia	Obowiązek zgłoszenia organowi nadzorcemu	Obowiązek zawiadomienia osoby, której dane dotyczą	Okoliczności naruszenia	Skutki naruszenia	Podjęte działania zaradcze

D Y R E K T O R
ZARZĄDU DROGOWEGO
[Signature]
inż. Ewa Kucharska

ZARZĄD DROGOWY
w Sępólnie Kraj.
Powiat Sępoleński
ul. Korcnowska 5
89-400 Sępólno Krajeńskie
tel. (052) 388 12 62
NIP 561-133-56-37 Regon 692353449