W systemie „CZD" przetwarzane są następujące dane dotyczące spersonalizowanej karty miejskiej: imię, nazwisko właściciela karty, jego adres zamieszkania i numer PESEL, numer wniosku o wydanie karty miejskiej, uprawnienia do przysługującej ulgi, opcjonalnie odnotowywany jest adres e-mail oraz numer telefonu właściciela karty. System odnotowuje również dane o okresie ważności, typie i rodzaju biletu zakodowanego na e-karcie - przykładowy wniosek o wydanie spersonalizowanej karty miejskiej stanowi załącznik B6.

Dane osobowe o właścicielu karty są pozyskiwane na podstawie danych zamieszczonych przez wnioskodawcę na formularzu wniosku o wydanie e-karty miejskiej. Wniosek taki musi być wypełniony przez wnioskodawcę w postaci papierowej, wnioski w postaci elektronicznej nie są w ZTZ Rybnik obsługiwane. W procesie produkcji karty spersonalizowanej pozyskiwane jest, poprzez skanowanie, zdjęcie wnioskodawcy. Istnieje możliwość pobrania formularza o wydanie spersonalizowanej karty miejskiej zamieszczonego na stronie internetowej pod adresem ekarta.rybnik.eu, jednak wniosek taki musi być złożony do ZTZ w formie papierowej. W przypadku, gdy wnioskodawca złoży wniosek o wydanie spersonalizowanej karty miejskiej jego dane są wprowadzane do systemu „CZD" w sposób manualny, przez pracowników z uprawnieniami do personalizacji.

Zakres danych zapisanych na chipie spersonalizowanej karty miejskiej to: numer karty, imię i nazwisko, numer PESEL użytkownika karty, (np. student, emeryt), rodzaj i typ biletu oraz okres ważności biletu. Dane nadrukowane na spersonalizowanej karcie miejskiej to: imię i nazwisko właściciela karty oraz jego zdjęcie.

Zakres danych osobowych przetwarzanych w systemie informatycznym w związku z obsługą spersonalizowanej karty miejskiej (w systemie „CZD") obejmuje dane wskazane na zrzutach ekranu z systemu „CZD", które stanowią załącznik B13.

Pan S.W. (art.5 ust. 2 ustawy wyjaśnił, że zakres danych przedstawiany w załączniku B13 to zakres danych, które kodowane są na spersonalizowanej karcie miejskiej.

Ponadto, ustalono, iż numer PESEL jest przetwarzany w systemie informatycznym „CZD" w celu wykonania jednoznacznej identyfikacji osoby (pasażera). Stanowisko ZTZ w zakresie wskazania podstaw prawnych przetwarzania numeru PESEL przedstawione zostało w piśmie, stanowiącym załącznik B12.

Ponadto w systemie informatycznym „CZD" obsługiwana jest „dualna" stykowa karta chipowa, która użytkowana jest m.in. jako spersonalizowana karta miejska. Służy ona przede wszystkim do składania niekwalifikowanego podpisu elektronicznego, lecz może pełnić również funkcję spersonalizowanej karty miejskiej. Jest to karta „dualna", która posiada wbudowany podwójny mikroprocesor (chip). Na chipie stykowym zapisane są dane dotyczące podpisu elektronicznego.

a na chipie zbliżeniowym dane dotyczące funkcji karty miejskiej. W systemie „CZD" wykonywana jest, na zlecenie Urzędu Miasta, personalizacja takich kart (dotyczy to jedynie programowania mikroprocesora zbliżeniowego, gdzie zapisywane są dane dotyczące e-karty). Zakres danych przetwarzanych na tej karcie (w przypadku, gdy pełni ona rolę karty miejskiej) jest taki sam, jak dla spersonalizowanej karty miejskiej. Pan S.W. (art.5 ust. 2 ustawy wyjaśnił, że ZTZ nie posiada dostępu do danych zapisanych na chipie, który wykorzystywany jest na karcie „dualnej" jako nośnik danych dla funkcji składania podpisu elektronicznego i dlatego zakres przetwarzanych na tym chipie danych nie jest mu znany. Dostęp do danych przetwarzanych na tej karcie w zakresie jej funkcji składania podpisu elektronicznego posiada Urząd Miasta Rybnika.

Pan S.W. (art.5 ust. 2 ustawy wyjaśnił, że usunięcie danej o numerze PESEL zakodowanej na spersonalizowanej karcie miejskiej jest możliwe do wykonania z poziomu systemu „CZD".

Administratorem danych osobowych jest Urząd Miasta Rybnika, serwer systemu znajduje się w siedzibie tego Urzędu. Dostęp do danych przetwarzanych w tym systemie posiadają jedynie pracownicy ZTZ oraz pracownicy Urzędu Miasta Rybnika. Ww. Administrator danych decyduje o zakresie uprawnień, jaki przyznawane są użytkownikom tego systemu informatycznego, w tym nadaje on uprawnienia dla pracowników ZTZ, którzy użytkują ten system.

System informatyczny o nazwie „CZD" umożliwia odnotowanie daty wprowadzenia danych do systemu informatycznego oraz identyfikatora użytkownika, który wprowadził dane do systemu.

Sporządzenie raportu w zakresie udokumentowania ww. odnotowań nie jest możliwe do wykonania z poziomu użytkownika tego systemu zatrudnionego w ZTZ. Nie pozwala na to poziom posiadanych przez tych pracowników uprawnień. Raport taki może sporządzić pracownik Urzędu Miasta.

Pan S.W. art. 5 ust. 2 ustawy wyjaśnił, że połączenie sieciowe pomiędzy komputerami ZTZ a serwerem systemu informatycznego „CZD" jest zestawione przy pomocy światłowodowego, szyfrowanego łącza art.5 ust. 2 utawy o dostępie do informacji publicznej

Dane osobowe, które zostały wprowadzone do systemu „CZD" nie są z tego systemu usuwane, chyba, że właściciel tych danych zgłosi pisemną prośbę o usunięcie tych danych.

Pan S.W. art. 5 ust. 2 wyjaśnił, że źródłem pozyskania danych osobowych w związku z wydaniem imiennej elektronicznej karty miejskiej są osoby ubiegające się o jej wydanie. Ustalono, iż system informatyczny o nazwie „CZD" nie umożliwia odnotowania informacji o źródle pozyskania danych, zatem nie umożliwia również sporządzenia raportu w tym zakresie.

Jak ustalono w toku kontroli dane osobowe przetwarzane w ww. systemach informatycznych użytkowanych ZTZ nie są udostępniane podmiotom zewnętrznym, poza Miejskimi Punktami Sprzedaży, które zajmują się obsługą e-karty w zakresie doładowania e-karty biletem okresowym

i punktami na przejazdy jednorazowe. Miejskie Punkty Sprzedaży funkcjonują w strukturze jednostek Urzędu Miasta. Ustalono również, że w MPS-ach istnieje dostęp do systemu „CZD", do pełnego zakresu danych przetwarzanych w tym systemie.

Dostęp do ww. wymienionych systemów informatycznych posiadają upoważnieni pracownicy ZTZ oraz pracownicy MPS-ów, w zakresie nadanych uprawnień przez Urząd Miasta Rybnika. Kserokopie pięciu przykładowych upoważnień do przetwarzania danych osobowych dla pracowników ZTZ Rybnik stanowią załącznik B7.

W ZTZ prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych. Kserokopia powołanej ewidencji stanowi załącznik B8.

W ZTZ zostały opracowane i wdrożone następujące dokumenty: „Polityka bezpieczeństwa Zarządu Transportu Zbiorowego w Rybniku" oraz „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Zarządzie Transportu Zbiorowego w Rybniku". Kserokopie ww. powołanych dokumentów stanowią odpowiednio załączniki B9 i B10. Kserokopia Zarządzenia wewnętrznego 7 2006 w sprawie wprowadzenia polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" z dnia 30 października 2006 r. stanowi załącznik B11.

Jak wyjaśnił Pan S.W. art. 5 ust. 2 (protokół przyjęcia ustnych wyjaśnień stanowi załącznik B14): komputery pracujące w systemie informatycznym „CZD" nie posiadają dostępu do sieci publicznej.

W ZTZ został wyznaczony administrator bezpieczeństwa informacji - kserokopia stosownego pisma w tej sprawie stanowi załącznik B15.

Jak wynika z zasad wskazanych w polityce bezpieczeństwa obszar przetwarzania danych osobowych w ZTZ zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.

Ww. polityka określa również zasady przebywania osób nieuprawnionych w obszarze przetwarzania danych osobowych.

W systemach informatycznych używanych w ZTZ do przetwarzania danych osobowych zapewnia się, aby: rejestrowany był dla każdego użytkownika odrębny identyfikator; dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

Systemy te zabezpiecza się, w szczególności przed: działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego (w tym celu w systemach informatycznych zainstalowano oprogramowanie antywirusowe (art. 5 ust. 2 ustawy o dostępie do informacji)) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci

zasilającej. Serwery znajdujące się w serwerowni, w siedzibie ZTZ Rybnik są zabezpieczone centralnym urządzeniem UPS.

Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie jest przydzielony innej osobie. Wynika to z przyjętych zasad przetwarzania danych osobowych, które zostały wskazane w polityce bezpieczeństwa. Dane osobowe przetwarzane w systemach informatycznych używanych w ZTZ do przetwarzania danych osobowych zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych. Dotyczy to systemu „Rewizor 2000". Dla pozostałych systemów informatycznych użytkowanych w ZTZ w związku z obsługą spersonalizowanej karty miejskiej kopie zapasowe nie są wykonywane, gdyż zasoby informatyczne i dane znajdują się poza siedzibą ZTZ, tj. w Urzędzie Miasta w Rybniku. S.W. art. 5 ust. 2 ustawy wyjaśnił, że z posiadanych przez niego informacji wynika, iż kopie zapasowe tworzone są przez administratora danych tj. przez Urząd Miasta w Rybniku.

Kopie zapasowe dla systemu „Rewizor 2000" przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem. Ww. kopie usuwa się niezwłocznie po ustaniu ich użyteczności. Kopie zapasowe systemu „Rewizor 2000" wykonywane są codziennie na dysku komputera, na którym użytkowany jest aplikacja systemu „Rewizor 2000". Kopia jest zapisywana jako ukryty katalog i użytkownik stacji nie ma dostępu do tej kopii. Dane przetwarzane w tym systemie informatycznym znajdują się na delegowanym serwerze, który jest zlokalizowany w serwerowni ZTZ Rybnik. Baza danych tego systemu informatycznego to SQL Server 2000.

Ustalono również, iż komputery przenośne nie są użytkowane w ZTZ do przetwarzania danych osobowych.

Ponadto, w toku kontroli ustalono, iż urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;

przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;

- naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

Ponadto monitorowane są wdrożone zabezpieczenia systemów informatycznych poprzez kontrolę wpisów w dziennikach zdarzeń poszczególnych systemów, logi systemu antywirusowego.

W przypadku zastosowania logicznych zabezpieczeń obejmują one:

a) kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną;

b) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych.

Pan S.W. (art. 5 ust. 2 ustawy) wyjaśnił, że urządzenia i nośniki zawierające dane osobowe, nie są przekazywane poza obszar przetwarzania danych osobowych.

System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.

Do połączenia pomiędzy ZTZ a Urzędem Miasta w Rybniku wykorzystana jest delegowana linia przesyłowa (szyfrowane łącze W celu zabezpieczenia dostępu do ww. sieci zastosowano routery dostępowe art.5 ust. 2 ustawy o dostępie do infromacji publicznej

W toku czynności kontrolnych dokonano oględzin miejsca, pomieszczeń oraz urządzeń, nośników, systemów informatycznych służących do przetwarzania danych osobowych znajdujących się w pomieszczeniu, gdzie wykonywana jest personalizacja e-karty (protokół oględzin stanowi załącznik B16), w wyniku których ustalono co następuje: jest to wydzielone pomieszczenie znajdujące się w siedzibie ZTZ Rybnik.

(art. 5 ust.2 ustawy o dostępie do infromacji publicznej

Dostęp do ww. komputera jest autoryzowany - wymagane jest wykonanie logowania do systemu operacyjnego MS Windows XP oraz logowanie do aplikacji systemu „CZD".

art. 5 ust. 2 ustawy o dostępie do informacji publicznej

Komputer chroniony jest przez

W toku czynności kontrolnych dokonano oględzin miejsca, pomieszczeń oraz urządzeń, nośników, systemów informatycznych służących do przetwarzania danych osobowych znajdujących się pomieszczeniu, gdzie na jednym komputerze PC obsługiwany jest system „Rewizor 2000" (protokół oględzin stanowi załącznik B17), w wyniku których ustalono co następuje: jest to wydzielone pomieszczenie znajdujące się na pierwszym piętrze, w siedzibie ZTZ.

W ww. pomieszczeniu znajduje się komputer umożliwiający dostęp do systemu „Rewizor 2000", na którym wykonywana jest obsługa mandatów za przejazdy wykonane bez wymaganych uprawnień oraz obsługa windykacyjna. Komputer ten pracuje pod kontrolą systemu operacyjnego MS Windows XP z zainstalowanym dodatkiem serwisowym SP2.

Dostęp do ww. komputera jest autoryzowany -

Ww. komputer nie posiada dostępu do sieci Internet.

W toku czynności kontrolnych dokonano oględzin miejsca, pomieszczeń oraz urządzeń, nośników, systemów informatycznych służących do przetwarzania danych osobowych znajdujących się w serwerowni systemów informatycznych użytkowych w Zarządzie Transportu Zbiorowego (protokół oględzin stanowi załącznik B25), w wyniku których ustalono, co następuje: serwerownia systemów informatycznych użytkowanych w ZTZ Rybnik jest zlokalizowana na pierwszym piętrze, w siedzibie ZTZ.

Dostęp osób postronnych (pracowników serwisu) do serwerowni jest ograniczony, a osoby takie mogą przebywać w serwerowni jedynie w obecności osoby upoważnionej.