ZARZĄDZENIE NR 736/13
BURMISTRZA STRONIA ŚLĄSKIEGO

z dnia 5 września 2013 r.

w sprawie zmiany zarządzenia nr 115/11 Burmistrza Stronia Śląskiego z dnia 21 czerwca 2011 r. w sprawie wprowadzenia do użytku służbowego „Polityki bezpieczeństwa informacji" oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" w Urzędzie Miejskim w Stroniu Śląskim.

Na podstawie art. 31 oraz art. 33 ust. 3 w związku z art. 11a ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (j.t. Dz.U. z 2013 r., poz. 594 ze zmianami) i art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 ze zmianami) oraz § 1 pkt 1 w związku z § 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. Nr 100, poz.1024.), **Burmistrz Stronia Śląskiego zarządza co następuje:**

§ 1. 1. Załącznik nr 1 do zarządzenia Nr 115/11 Burmistrza Stronia Śląskiego z dnia 21 czerwca 2011 roku „Polityka bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miejskim w Stroniu Śląskim" otrzymuje brzmienie zgodne z załącznikiem nr 1 do niniejszego zarządzenia.

2. Załącznik nr 2 do zarządzenia Nr 115/11 Burmistrza Stronia Śląskiego z dnia 21 czerwca 2011 roku „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Stroniu Śląskim" otrzymuje brzmienie zgodne z załącznikiem nr 2 do niniejszego zarządzenia.

3. Załącznik nr 3 do zarządzenia Nr 115/11 Burmistrza Stronia Śląskiego z dnia 21 czerwca 2011 roku - wykaz zbiorów oraz programów służących do ich przetwarzania wraz ze strukturą przetwarzanych danych otrzymuje brzmienie zgodne z załącznikiem nr 3 do niniejszego zarządzenia.

§ 2. Wykonanie zarządzenia powierza się Sekretarzowi Gminy Stronie Śląskie.

§ 3. Zarządzenie wchodzi w życie z dniem podjęcia.

Burmistrz

Zbigniew Łopusiewicz

Załącznik nr 1 do Zarządzenia Nr 736/13
Burmistrza Stronia Śląskiego
z dnia 05 września 2013 r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI URZĘDU MIEJSKIEGO W STRONIU ŚLĄSKIM

W celu zabezpieczenia danych gromadzonych i przetwarzanych w Urzędzie Miejskim w Stroniu Śląskim oraz jego systemie informatycznym, a w szczególności w celu ochrony danych osobowych, wprowadza się określone w niniejszym dokumencie zasady bezpieczeństwa.

Mając świadomość, że żadne zabezpieczenie techniczne nie gwarantuje 100%-towej szczelności systemu, konieczne jest, aby każdy pracownik pełen świadomej odpowiedzialności, postępował zgodnie z przyjętymi zasadami i minimalizował zagrożenia wynikające z ludzkich błędów.

Podstawa prawna.

1. Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 ze zmianami).
2. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. Nr 100, poz. 1024).

Definicje

Ilekroć w niniejszym dokumencie jest mowa o:

1. **Urzędzie** - należy przez to rozumieć Urząd Miejski w Stroniu Śląskim.
2. **Administratorze Danych** - należy przez to rozumieć Burmistrza Stronia Śląskiego.
3. **Administratorze Bezpieczeństwa Informacji** - należy przez to rozumieć pracownika urzędu lub inna osobę wyznaczona do nadzorowania przestrzegania zasad ochrony określonych w niniejszym dokumencie oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych.
4. **Administratorze Systemu Informatycznego** należy przez to rozumieć osobę odpowiedzialną za funkcjonowanie systemu informatycznego urzędu oraz stosowanie technicznych i organizacyjnych środków ochrony.
5. **Systemie informatycznym** - należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji narzędzi programowych zastosowanych w celu przetwarzania danych.
6. **Użytkowniku systemu** - należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym urzędu. Użytkownikiem może być pracownik urzędu, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno prawnej, osoba odbywająca staż w urzędzie, wolontariusz.
7. **Sieci lokalnej** - należy przez to rozumieć połączenie systemów informatycznych urzędu wyłącznie dla własnych jej potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych.
8. **Sieci rozległej** - należy przez to rozumieć sieć publiczną w rozumieniu ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz.U. z 2004 r. Nr 171, poz. 1800, ze zmianami).
9. **Zbiorze danych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
10. **Przetwarzanie danych** - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.
11. **Zabezpieczenie danych w systemie informatycznym** wdrożenie i eksploatacja stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
12. **Identyfikator użytkownika** - ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

13. **Hasło** - ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
14. **Uwierzytelnianie** - działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
15. **Rozliczalność** - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
16. **Integralność danych** - właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
17. **Poufność danych** - właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym osobom.

Polityka bezpieczeństwa określa.

1. Wykaz budynków oraz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe.
2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.
3. Opis struktury zbiorów danych wskazujących zawartości poszczególnych pól informacyjnych.
4. Sposób przepływu danych pomiędzy systemami – struktura powiązań systemów.
5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności i rozliczalności przetwarzanych danych.

Ad. 1.
Obszar przetwarzania danych osobowych.

Miejscem przetwarzania danych osobowych są pomieszczenia pracy komórek organizacyjnych Urzędu Miejskiego w Stroniu Śląskim, Gminnego Centrum Informacji w Stroniu Śląskim oraz Straży Miejskiej w Stroniu Śląskim.

Wykaz budynków oraz pomieszczeń stanowiących obszar przetwarzania danych osobowych.

Lp.	Adres - budynek	Numery pomieszczeń
1	Stronie Śląskie, ul. Kościuszki 55 - Urząd Miejski w Stroniu Śląskim	2,3,4,5,8,9,11,12,13,14,15,17,19,20,24,25,26,27
2	Stronie Śląskie, ul. Kościuszki 32 - Gminne Centrum Informacji w Stroniu Śląskim (budynek Biblioteki Miejskiej)	
3	Stronie Śląskie, ul. Mickiewicza 2 - Straż Miejska w Stroniu Śląskim	

Ad.2

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

Za zbiór danych osobowych przetwarzanych w Urzędzie Miejskim w Stroniu Śląskim uważa się:

1. dokumentację papierową (korespondencja, wnioski, deklaracje, itd.),
2. systemy informatyczne przetwarzania danych oraz oprogramowanie komputerowe służące do przetwarzania informacji,
3. wydruki komputerowe.

Wykaz zbiorów oraz programów służących do ich przetwarzania określa załącznik nr 3 do zarządzenia nr 115/11 Burmistrza Stronia Śląskiego z dnia 21 czerwca 2011 r.

Ad. 3. Ad. 4.

Opis struktury zbiorów danych osobowych oraz sposób przepływu danych pomiędzy systemami informatycznymi został wskazany w dokumentacji technicznej dostarczonej przez producenta systemów Radix. Dokumentacja jest dostępna do wglądu u Administratora Systemów Informatycznych w Urzędzie Miejskim w Stroniu Śląskim.

Struktura powiązań systemów informatycznych Radix zawarta jest w załączniku nr 3 do zarządzenia nr 115/11 Burmistrza Stronia Śląskiego z dnia 21 czerwca 2011 r.

Ad. 5.

Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

A. Dane w postaci elektronicznej.

Dane przetwarzane są przy użyciu komputerów pracujących wyłącznie w wewnętrznej sieci komputerowej oddzielonej fizycznie od sieci publicznej przy pomocy bramy internetowej wyposażonej w firewall oraz programowe firewalle na stacjach roboczych, dodatkowo zabezpieczonych oprogramowaniem antywirusowym.

Dostęp do danych następuje po autoryzacji. Autoryzacja polega na podaniu identyfikatora oraz hasła przydzielonego przez Administratora Bezpieczeństwa Informacji na podstawie zgody Administratora Danych.

Uwzględniając kategorie przetwarzanych danych wprowadza się podstawowy poziom bezpieczeństwa. Środki bezpieczeństwa na poziomie podstawowym określa instrukcja zarządzania systemem informatycznym.

B. Dane w rejestrach papierowych.

Dane przetwarzane przy użyciu tradycyjnych środków pisarskich gromadzone są w rejestrach, księgach, zeszytach papierowych oraz segregatorach i przechowywane w zamykanych szafach oraz kasach pancernych.

C. Środki organizacyjne.

Administrator Danych powołuje Administratora Bezpieczeństwa Informacji (ABI), który nadzoruje przestrzeganie zasady ochrony danych określonych w instrukcji zarządzania systemem informatycznym z uwzględnieniem spraw dotyczących ochrony danych osobowych przetwarzanych w tradycyjnych rejestrach.

D. Środki organizacyjne oraz środki ochrony fizycznej.

1. Wejście do budynku Urzędu Miejskiego zabezpieczone winno być zamkami drzwiowymi oraz alarmem. Poszczególne pokoje, w których odbywa się przetwarzanie danych osobowych i ich składowanie muszą być wyposażone w niezależne zamki i muszą być zamykane podczas nieobecności pracownika. Odpowiedzialność za właściwą ochronę pomieszczeń ponosi pracownik oraz kierownik komórki organizacyjnej.
2. Przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych dopuszczalne jest tylko w obecności osoby zatrudnionej przy przetwarzaniu danych lub w obecności Administratora Bezpieczeństwa Informacji.
3. Pomieszczenia, o których mowa wyżej, zamykane są na czas nieobecności pracownika zatrudnionego przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich. Klucze do pomieszczeń służbowych znajdują się w budynku Urzędu w Biurze Obsługi Klienta. Pozostawienie kluczy w zamkach pomieszczeń gdzie przetwarzane są dane osobowe jest niedopuszczalne (także podczas pobytu pracownika w pokoju).
4. W pomieszczeniach, w których przewiduje się przyjmowanie interesantów monitory stanowisk komputerowych ustawione są w sposób uniemożliwiający wgląd w przetwarzane dane.
5. Pracownicy przetwarzający dane osobowe obowiązani są do prawidłowego ich zabezpieczenia na swoich stanowiskach pracy. Przed rozpoczęciem pracy klucze pobierane

zostają z zabezpieczonej gabloty pod nadzorem pracownika Biura Obsługi Klienta i tam też składowane po zakończeniu pracy.

E. Środki sprzętowe, informatyczne i telekomunikacyjne.

1. Urządzenia wychodzące w skład systemu informatycznego podłączone są do odrębnego obwodu elektrycznego, zabezpieczonego na wypadek zaniku napięcia albo awarii w sieci zasilającej listwą filtrującą oraz urządzeniem UPS.
2. Dostęp fizyczny do sieci lokalnej jest ograniczony, koncentrator umieszczony jest w specjalnie przygotowanej zamykanej szafie.
3. Dostęp logiczny do sieci lokalnej zabezpieczony jest adresem IP oraz MAC - adresem karty sieciowej.
4. Dostęp do sieci WAN zabezpieczony jest Firewall-em wraz z oprogramowaniem antywirusowym.
5. Kopie awaryjne wykonywane są w cyklach:

    - dzienna na dysku twardym – narastająco do 30 dni,
    - kwartalnie na nośniku zewnętrznym.

6. Każdy dokument papierowy zawierający dane osobowe przeznaczony do wyrzucenia zostaje zniszczony w sposób uniemożliwiający jego odczytanie przy pomocy niszczarki.
7. Inne środki przetwarzania: drukarki, skanery, modemy, niszczarki dokumentów.

F. Środki ochrony w ramach oprogramowania.

1. Każda jednostka komputerowa zabezpieczona została hasłem wejściowym do systemu operacyjnego połączonego z profilem użytkownika na serwerze oraz odrębnym identyfikatorem i hasłem do każdej aplikacji przy pomocy, której przetwarzane są dane osobowe.
2. Zastosowano wygaszanie ekranu w przypadku dłuższej nieaktywności użytkownika.
3. Zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji.
4. Dla każdego użytkownika systemu jest ustalony odrębny identyfikator.
5. Zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (unikalny identyfikator i hasło).
6. Hasła do aplikacji zmieniane są co 30 dni.

<u>Do zapoznania się z niniejszym dokumentem oraz stosowania zawartych w nim zasad zobowiązani są wszyscy pracownicy urzędu upoważnieni do przetwarzania danych osobowych.</u>

Załącznik nr 2 do Zarządzenia Nr 736/13
Burmistrza Stronia Śląskiego
z dnia 05 września 2013 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI W URZĘDZIE MIEJSKIM W STRONIU ŚLĄSKIM

I. Procedury nadawania i zmiany uprawnień do przetwarzania danych.

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych jest zobowiązany do zapoznania się:
   - ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych,
   - polityką bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miejskim w Stroniu Śląskim,
   - instrukcją zarządzania systemami informatycznymi w Urzędzie Miejskim w Stroniu Śląskim.

2. Administrator Bezpieczeństwa Informacji przyznaje uprawnienia w zakresie dostępu do systemu informatycznego poszczególnym pracownikom urzędu za pośrednictwem Administratora Systemów Informatycznych.
3. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora, hasła oraz zakresu dostępnych danych i operacji.
4. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.
5. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.
6. Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą jako naruszenie podstawowych obowiązków pracowniczych.
7. Pracownik zatrudniony przy przetwarzaniu danych osobowych zobowiązany jest do zachowania ich w tajemnicy. Tajemnica obowiązuje go również po ustaniu zatrudnienia.
8. Odebranie uprawnień pracownikowi następuje na pisemny wniosek kierownika, któremu pracownik podlega z podaniem daty oraz przyczyny odebrania uprawnień.

9. Kierownicy komórek organizacyjnych zobowiązani są pisemnie informować Administratora Bezpieczeństwa Informacji o wszelkich zmianach kadrowych mających wpływ na zakres posiadanych uprawnień w systemie informatycznym.
10. Identyfikator osoby, która utraciła uprawnienia dostępu do danych osobowych należy niezwłocznie wyrejestrować z systemu informatycznego oraz unieważnić jej hasło.
11. Administrator Bezpieczeństwa Informacji zobowiązany jest do prowadzenia rejestru użytkowników i ich uprawnień w systemie informatycznym.
13. Rejestr użytkowników i ich uprawnień w systemie informatycznym, powinien zawierać:
    - imię i nazwisko użytkownika systemów informatycznych,
    - rodzaj uprawnienia,
    - datę nadania uprawnienia,
    - datę odebrania uprawnienia,
    - przyczynę odebrania uprawnienia,
    - podpis Administratora Bezpieczeństwa Informacji.

II. Zasady posługiwania się hasłami.

1. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
2. Hasło użytkownika powinno być zmieniane co najmniej raz na trzy miesiące.
3. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.
4. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł.
5. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.
6. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
7. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła.

III. Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie.

1. Przed rozpoczęciem pracy w systemie komputerowym należy zalogować się do systemu przy użyciu indywidualnego identyfikatora oraz hasła.
2. Po opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy wyjść z programu.

3. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów oraz wykonać zamknięcie.
4. Niedopuszczalne jest zamknięcie komputera przed zamknięciem oprogramowania.

IV. Zasady instalacji oprogramowania.

1. Dopuszcza się instalację na serwerze nowego oprogramowania do przetwarzania danych osobowych lub aktualizacji istniejących pod warunkiem spełnienia określonych wymagań.
2. Instalacji dopuszczonych do użytkowania programów do przetwarzania danych osobowych lub ich aktualizacji dokonuje Administrator Systemów Informatycznych lub osoba przez niego upoważniona. Rejestr instalacji oprogramowania prowadzi Administrator Systemów Informatycznych, dane dotyczące aktualizacji poszczególnych programów zawarte są w historii zmian każdego programu.
3. Na wszystkich komputerach Urzędu Miejskiego w Stroniu Śląskim dopuszcza się instalację tylko legalnego, licencjonowanego oprogramowania.
4. Zabrania się instalowania oprogramowania bez zgody Administratora Bezpieczeństwa Informacji.

V.Procedury tworzenia zabezpieczeń.

1. Za systematyczne przygotowanie kopii bezpieczeństwa odpowiada Administrator Systemu Informatycznego.
2. Kopie bezpieczeństwa wykonywane są w systemie dziennym na dysk twardy narastająco do 30 dni oraz raz na kwartał na nośnik zewnętrzny.
3. Nośnik z kopiami bezpieczeństwa przechowywane są w zamykanej szafie u Administratora Systemów Informatycznych.
4. Na każdym stanowisku komputerowym oraz serwerze zainstalowane jest oprogramowanie antywirusowe pracujące w trybie monitora.
5. Zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym.
6. Zabrania się pobierania plików z Internetu niewiadomego pochodzenia.
7. Administrator Systemu Informatycznego przeprowadza cyklicznie kontrole antywirusowe na wszystkich komputerach - minimum raz na miesiąc.

VI. Zasady dokonywania napraw.

1. Dokonywanie napraw, przeglądów i konserwacji systemu przez pracowników serwisu mogą odbywać się jedynie w obecności Administratora Bezpieczeństwa Informacji lub osoby przez niego upoważnionej.
2. Przeglądów należy dokonywać nie rzadziej niż raz na kwartał.
3. Fakt dokonania naprawy, przeglądów lub konserwacji musi być udokumentowany w dokumentacji systemu.
4. Uszkodzone nośniki magnetyczne lub inne zawierające dane osobowe nie mogą być użytkowane. Muszą być odpowiednio zabezpieczone przed nieuprawnionym udostępnieniem, a następnie zniszczone lub naprawione pod nadzorem osoby upoważnionej przez Administratora Danych.

VII. Nośniki papierowe danych - wydruki.

1. W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym.
2. Pomieszczenie, w którym przechowywane są wydruki robocze musi być należycie zabezpieczone po godzinach pracy.
3. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

VIII. Profilaktyka antywirusowa.

1. Każdy użytkownik komputera w urzędzie gminy zobowiązany jest do używania w pracy dyskietek i płyt CD zakupionych przez urząd (nie prywatnych).
2. Informacje i dane przechowywane na dyskietkach i płytach CD mogą mieć wyłącznie charakter związany z pracą.
3. Każdy komputer minimum raz w tygodniu powinien zostać sprawdzony aktualną wersją programu antywirusowego.
4. Dyskietki lub płyty CD przekazywane Urzędowi Miejskiemu mogą być odczytywane na komputerach, ***tylko i wyłącznie po wcześniejszym sprawdzeniu programem antywirusowym.***

IX. Zasady korzystania z Internetu.

Przy korzystaniu z Internetu w Urzędzie Miejskim w Stroniu Śląskim należy stosować następujące zasady:

1. Pracownicy mogą korzystać z dostępu do Internetu tylko i wyłącznie w celach służbowych, tj. w zakresie:
    a. poszukiwania wyjaśnień i interpretacji przepisów prawnych,
    b. komunikacji i pozyskiwania informacji z innych urzędów administracji rządowej jak i samorządowej wynikające z wykonywanych obowiązków służbowych,
    c. przeglądania stron — Biuletynów Informacji Publicznej prowadzonych w oparciu o przepisy ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. Nr 112, poz. 1198, ze zmianami),
    d. kopiowania danych wykorzystywanych wyłącznie do celów służbowych o ile nie jest to sprzeczne z prawem autorskim.
2. Niedozwolone jest:
    a. kopiowanie na dysk twardy komputera danych oraz instalacji programów dostępnych na serwerach internetowych,
    b. użytkowanie jakichkolwiek programów niezwiązanych z wykonywanymi obowiązkami służbowymi,
    c. odwiedzanie popularnych serwisów i wszystkich innych stron (np. Nasza klasa, Allegro, Ceneo itp.), które nie zawierają treści pomocnych przy wykonywaniu obowiązków służbowych,
    d. realizacji swoich własnych spraw np. (zakupy, wysyłanie osobistych e-maili z własnych skrzynek pocztowych, dokonywanie przelewów (płatności) z rachunków osobistych)),
    e. grania w popularne gry dostępne w Internecie.

Załącznik nr 3 do Zarządzenia Nr 736/13
Burmistrza Stronia Śląskiego
z dnia 05 września 2013 r.

Wykaz zbiorów oraz programów służących do ich przetwarzania wraz ze strukturą przetwarzanych danych

Nazwa zbioru	Osoba odpowiedzialna	Program	Struktura przetwarzanych danych
Dzierżawcy nieruchomości zabudowanych i niezabudowanych stanowiących własność Gminy Stronie Śląskie	Halina Czerhoniak	Rejestr prowadzony ręcznie w formie papierowej	Imię, nazwisko, adres zamieszkania, adres miejsca dzierżawy
Rejestr kwater grzebalnych	Halina Czerhoniak	Rejestr prowadzony ręcznie w formie papierowej	Imię, nazwisko, osoby zmarłej, data i miejsce urodzenia oraz zgonu, przyczyna zgonu, ostatnie miejsce zamieszkania
Rejestr sprzedaży, nabycia i zamiany nieruchomości	Urszula Czyżewska	Rejestr prowadzony ręcznie w formie papierowej	Imię, nazwisko, adres zamieszkania, położenie działki, powierzchnia, akt notarialny
Rejestr właścicieli psów	Józef Kałużny	Rejestr prowadzony ręcznie w formie papierowej + wersja elektroniczna (program Word)	Imię, nazwisko, adres zamieszkania właściciela
Umowy najmu lokali komunalnych	Halina Czerhoniak / Józef Kałużny	Rejestr prowadzony ręcznie w formie papierowej + wersja elektroniczna (program Word)	Imię, nazwisko, adres zamieszkania, powierzchnia, skład mienia, wys. czynszu
Ewidencja działalności gospodarczej	Anna Sporek	Radix/ EPOD, EPODX	Imię, nazwisko, adres zamieszkania i wykonywania dz.gosp., nr tel, konto bankowe, pełnomocnictwo (dane osobowe osób upoważnionych)
Ewidencja zezwoleń na sprzedaż napojów alkoholowych	Anna Sporek	Radix/ALK	Imię, nazwisko, adres zamieszkania, adres lokalu, tytuł własności lokalu, pełnomocnictwo (dane osobowe osób upoważnionych)
Rejestr osób uzależnionych od alkoholu i narkomani	Anna Sporek	Rejestr prowadzony ręcznie w formie papierowej	Imię, nazwisko, adres zamieszkania

Rejestracja i kwalifikacja wojskowa	Agata Snopkowska	Radix/ELUD	Imię, nazwisko, nazwisko rodowe, adres zamieszkania, imiona i nazwiska rodziców, data i m-ce urodzenia, PESEL, seria i nr DO
Ewidencja ludności i dowodów osobistych	Agata Snopkowska/ Edyta Szkudlarek	Radix/ELUD, System Wydawania Dowodów Osobistych	Imię, nazwisko, adres zamieszkania, PESEL, data i m-ce urodzenia, imię i nazwisko małżonk-a/i, imiona i nazwiska rodziców, seria i nr DO
Rejestr Wyborców	Agata Snopkowska	Radix/WYB	Imię, nazwisko, adres zamieszkania, data urodzenia, PESEL
Urząd Stanu Cywilnego	Edyta Szkudlarek	Radix/USC	Imię, nazwisko, adres zamieszkania, PESEL, seria i nr DO, imiona i nazwiska rodziców
Ewidencja podatników, płatników i dłużników	Andrzej Konarski	Radix/POGRUN/WIP	Imię, nazwisko, adres zamieszkania, PESEL, NIP, dane dotyczące nieruchomości
Kadry i płace	Elżbieta Biegańska/ Jadwiga Mościszko	Radix/KADRY PŁACE, PŁATNIK	Imię, nazwisko, adres zamieszkania, PESEL, NIP, seria i nr DO, data i m-ce urodzenia, imiona i nazwiska rodziców
Rejestr wydanych decyzji o środowiskowych uwarunkowaniach realizacji przedsięwzięcia	Leszek Sadowski	Rejestr prowadzony ręcznie w formie papierowej	Imię, nazwisko, adres zamieszkania,
Rejestr wydanych decyzji o warunkach zabudowy i zagospodarowania terenu	Leszek Sadowski	Rejestr prowadzony ręcznie w formie papierowej	Imię, nazwisko adres zamieszkania, nazwa jednostki z adresem
Ewidencja zezwoleń na regularny przewóz osób w krajowym transporcie drogowym	Leszek Kawecki	Rejestr prowadzony ręcznie w formie papierowej	Imię, nazwisko, adres zamieszkania
Rejestr decyzji na zajęcie pasa drogowego drogi gminnej	Leszek Kawecki	Rejestr prowadzony ręcznie w formie papierowej	Imię, nazwisko, adres zamieszkania
Rejestr decyzji na usunięcie drzew lub krzewów	Leszek Kawecki	Rejestr prowadzony ręcznie w formie papierowej	Imię, nazwisko, adres zamieszkania

Ewidencja miejscowości, ulic i adresów Gminy Stronie Śląskie	Leszek Kawecki	Rejestr prowadzony ręcznie w formie papierowej	Imię, nazwisko, adres zamieszkania
Rejestr zezwoleń na prowadzenie działalności w zakresie odbierania odpadów	Leszek Kawecki	Rejestr prowadzony ręcznie w formie papierowej	Imię, nazwisko adres zamieszkania, nazwa jednostki z adresem
Decyzje w sprawie dofinansowania pracodawcom kosztów kształcenia młodocianych pracowników	Dariusz Chromiec	Rejestr prowadzony ręcznie w formie papierowej	Imię, nazwisko, adres zamieszkania, data i m-ce urodzenia, PESEL, dane pracodawcy z adresem
Decyzja w sprawie udzielenia dopłat do czesnego dla dokształcających się nauczycieli zatrudnionych w placówkach oświatowych	Dariusz Chromiec	Rejestr prowadzony ręcznie w formie papierowej	Imię, nazwisko, adres zamieszkania, data i m-ce urodzenia
Oświadczenia majątkowe radnych oraz osób zobowiązanych	Dariusz Chromiec	Rejestr prowadzony ręcznie w formie papierowej	Imię, nazwisko, adres zamieszkania, data i m-ce urodzenia, posiadany stan majątkowy
Realizacja obowiązku szkolnego i nauki przez uczniów szkół i placówek oświatowych	Dariusz Chromiec	Rejestr prowadzony ręcznie w formie papierowej	Imię, nazwisko, adres zamieszkania, data i m-ce urodzenia
Rejestr informacji publicznej	Tomasz Olszewski	Elektroniczny System Obiegu Dokumentów „Intradok”	Imię, nazwisko, adres zamieszkania
Użytkownicy wieczyści	Andrzej Konarski	Radix/EGW	Imię, nazwisko, adres zamieszkania
Rejestr wydanych decyzji o uznaniu żołnierza za posiadającego na wyłącznym utrzymaniu członków rodziny	Agata Snopkowska	Rejestr prowadzony ręcznie w formie papierowej	Imię, nazwisko, adres zamieszkania, data i m-ce urodzenia, imiona i nazwiska rodziców, miejsce pracy, zawód, wykształcenie
Świadczenia osobiste i rzeczowe na rzecz obrony	Agata Snopkowska	Rejestr prowadzony ręcznie w formie papierowej	Imię, nazwisko, adres zamieszkania, miejsce pracy, zawód, wykształcenie
Rejestr skarg i wniosków	Jadwiga Mościszko	Rejestr prowadzony ręcznie w formie papierowej	Imię, nazwisko, adres zamieszkania
Ewidencja wniosków do Centralnej Ewidencji i Informacji o Działalności Gospodarczej	Anna Sporek	Rejestr prowadzony w formie elektronicznej w programie Excel	Imię, nazwisko, adres zamieszkania, PESEL, NIP, seria i nr DO, data i m-ce urodzenia, imiona i nazwiska rodziców

Schemat powiązań między systemami komputerowymi, w których przetwarza się dane osobowe