ZARZĄDZENIE WEWNETRZNE NR 6/2010

Prezesa Zarządu Miejskiego Zakładu Gospodarki Komunalnej Sp. z o.o. w Nowej Soli
z dnia 30.08.2010

W sprawie : zatwierdzenia i przyjęcia do stosowania Polityki Bezpieczeństwa Informacji.

§1

W celu zapewnienia prawidłowego bezpieczeństwa informacji przyjmuje się do stosowania Politykę bezpieczeństwa, która stanowi Załącznik nr 1 do niniejszego zarządzenia wewnętrznego.

§2

Za wdrożenie Polityki Bezpieczeństwa odpowiada firma „Nova Komputery" w imieniu której działa p. Marek Śledzik, a za przestrzeganie jej postanowień kierownicy działów.

Do pełnienia funkcji Administratora Bezpieczeństwa Informacji został powołany Kierownik działu Administracyjno- Organizacyjnego – Pan Piotr Małek.

§3

Zobowiązuje się wszystkich pracowników korzystających z komputerów służbowych do zapoznania się z postanowieniami w/w Polityki i bezwzględnego jej stosowania.

§4

Zarządzenie wchodzi w życie z dniem podpisania.

PREZES ZARZĄDU

Waldemar Wrześniak

POLITYKA BEZPIECZEŃSTWA

Miejski Zakład Gospodarki Komunalnej w Nowej Soli 2010

§ 1.

DEFINICJA BEZPIECZEŃSTWA INFORMACJI

1. Stan bezpieczeństwa informacji to osiągnięcie uzasadnionych biznesowo poziomów poufności, integralności, dostępności, autentyczności i rozliczalności informacji tworzonej, przechowywanej, przetwarzanej i przesyłanej.
2. Aby osiągnąć ten stan Przedsiębiorstwo wdraża dokument „Instrukcja zarządzania systemem informatycznym", na który składa się zestaw praw, reguł i zasad ich tworzenia, sposobów zarządzania, dystrybucji, użytkowania i przechowywania danych osobowych.
3. Zarząd spółki wprowadza politykę bezpieczeństwa informacji w celu uświadomienia całej organizacji potrzeby ochrony danych niezależnie od przyjmowanej przez nie formy (dokumenty elektroniczne, wydrukowane).
4. Bezpieczeństwo systemów informatycznych odnosi się do wszystkich procesów związanych z informacją to jest: wytwarzania, przetwarzania, przechowywania, archiwizowania, przesyłania, zbierania, prezentowania oraz niszczenia.

§ 2.

OŚWIADCZENIE ZARZĄDU

1. Polityka Jakości MZGK nakłada na Przedsiębiorstwo obowiązek świadczenia usług na wysokim poziomie. Bezpieczeństwo informacji, w tym danych osobowych, ma znaczący wpływ na ten poziom.
2. Zarząd MZGK angażuje się w rozwój i wdrożenie systemu bezpieczeństwa danych osobowych posiadanych przez Przedsiębiorstwo. Zarząd deklaruje pracę nad stałym doskonaleniem niniejszej polityki.
3. Na wielu etapach przetwarzania danych najsłabszym ogniwem może być człowiek, dlatego Zarząd deklaruje, że będzie finansować szkolenia dla pracowników, które obejmować będą zagadnienia dotyczące zachowywania przetwarzanych przez MZGK zbiorów danych osobowych w bezpieczeństwie.

§ 3.

ZASADY, STANDARDY I WYMAGANIA ZGODNOŚCI

1. **Podstawa prawna:** dokument został stworzony na podstawie
   a. ustawy o ochronie danych osobowych z dnia 29 kwietnia 1997 roku z późniejszymi zmianami (Dz. U. 2002 nr 101 poz.926 tekst jednolity) zwanej dalej ustawą;
   b. rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. zwanego dalej rozporządzeniem [Dz. U.2004 nr 100 poz. 1024];
   c. ustawy z dnia 14.07.1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. Nr 97 z 2006 r. poz.673 z póź. zm.) oraz Rozporządzenia Ministra Kultury z dnia 16.09.2002r. (Dz.U. Nr 167/2002 z póź. zm.)
2. Mnogość zagrożeń nakłada na Przedsiębiorstwo obowiązek dbania o szkolenie pracowników w zakresie bezpieczeństwa informacji.
3. Za standard uważa się oprogramowanie antywirusowe i wykrywające szkodliwe oprogramowanie, w tym takie ustawienia oprogramowania użytkowego, które zminimalizują ryzyko zagrożenia stanu bezpieczeństwa. Samodzielne zmiany tych ustawień stanowią naruszenie zasad bezpieczeństwa.
4. Celem nadrzędnym jest zachowanie ciągłości działania biznesowego, dlatego w budżecie Przedsiębiorstwa zawsze znajduje się odpowiednia rezerwa finansowa na środki związane z ochroną informacji. Wysokość rezerwy ustalana jest na podstawie podanej przez Informatyka wartości szacunkowej w terminie do końca sierpnia każdego roku.
5. W związku z celami nadrzędnymi Przedsiębiorstwa zabrania się samowolnej instalacji oprogramowania i dopuszcza się kontrolę zawartości korespondencji firmowej.
6. Zabrania się używania komputerów firmowych do prywatnych celów w tym używania poczty prywatnej.
7. Oprócz prawnych konsekwencji naruszenia zasad polityki bezpieczeństwa wyróżnia się także konsekwencje marketingowe. Straty w obu kategoriach mogą być policzalne, zatem wszyscy pracownicy Przedsiębiorstwa muszą mieć świadomość tego faktu.

§ 4.

DEFINICJE POJĘĆ OGÓLNYCH I SZCZEGÓLNYCH OBOWIĄZKÓW W ODNIESIENIU DO ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

1. Pojęcia ogólne

1.1. **Dane osobowe** - każda informacja dotycząca osoby fizycznej pozwalająca na określenie tożsamości tej osoby.

1.2. **Przetwarzanie danych osobowych** – wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, udostępnianie i ich usuwanie.

1.3. **Administrator Bezpieczeństwa Informacji (ABI)** – osoba nadzorująca przestrzeganie zasad ochrony przetwarzania danych osobowych.

1.4. **Administrator Systemu Informatycznego i Sieci (ASiS)** – osoba fizyczna lub prawna odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemów oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w tych systemach (szef działu IT);

1.5. **Osoba upoważniona lub użytkownik systemu, zwany dalej użytkownikiem** – osoba posiadająca upoważnienie wydane przez Administratora Danych Osobowych (**ADO**) PREZES dopuszczona, w zakresie w nim wskazanym, jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej.

1.6. **Osoba trzecia** – każda osoba nieupoważniona i przez to nieuprawniona do dostępu do danych osobowych zbiorów będących w posiadaniu administratora danych. Osobą trzecią jest również osoba posiadająca upoważnienie wydane przez administratora danych podejmująca czynności w zakresie przekraczającym ramy jej upoważnienia.

1.7. **System informatyczny, zwany dalej systemem** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

1.8. **System operacyjny** - zespół współpracujących ze sobą programów, usług i narzędzi programowych potrzebnych do działania komputera.

1.9. **Zabezpieczenie systemu informatycznego** – wdrożenie przez Administratora Bezpieczeństwa Informacji (ABI) oraz Administratora Systemu Informatycznego i Sieci (ASiS) stosownych środków organizacyjnych i technicznych w celu zabezpieczenia zasobów oraz ochrony danych przed dostępem, modyfikacją ujawnieniem, pozyskaniem lub zniszczeniem przez użytkowników danych osobowych lub osobę trzecią.

2. Gromadzenie danych osobowych

2.1. Wszelkie dane osobowe gromadzone w MZGK są przetwarzane na podstawie zgody osób fizycznych których dane dotyczą lub na mocy umów z podmiotami zewnętrznymi (przeważnie organami administracji samorządowej lub rządowej).

2.2. Dane osobowe znajdujące się w posiadaniu MZGK są chronione w sposób zapewniający ich pełne bezpieczeństwo, w tym bezpieczeństwo przed utratą, kradzieżą bądź nieautoryzowanymi zmianami.

2.3. Każda osoba, której dane osobowe znajdują się w posiadaniu MZGK ma prawo przeglądać swoje dane oraz je modyfikować w celu ich uzupełnienia lub poprawy.

3. **Ochrona danych osobowych**
   3.1. W związku z bezpośrednim połączeniem sieci komputerowej z siecią publiczną dane przechowywane są w naszych bazach i zbiorach zabezpieczonych przed dostępem niepowołanych osób wg zaleceń ustawy o Ochronie Danych Osobowych na najwyższym poziomie bezpieczeństwa.
   3.2. Dla ochrony danych stworzono odpowiednie procedury zasad bezpieczeństwa. Procedury te opisane są w Instrukcji Zarządzania Systemem Informatycznym MZGK. Procedury pozwalają na przetwarzanie danych osobowych wyłącznie osobom, którym jest to niezbędne do wykonywania pracy. Osoby te są ewidencjonowane oraz posiadają upoważnienia do przetwarzania danych.
   3.3. Wszelkie informacje mogące zawierać dane osobowe są przechowywane w taki sposób, aby zminimalizować ryzyko ich ujawnienia, modyfikacji, zniszczenia lub utraty.
   3.4. Dane osobowe są zabezpieczane fizycznie (np. przed awarią sprzętu), jak i elektronicznie (np. przed atakiem hakera lub dostępem niepowołanych osób).
   3.5. Dane osobowe przetwarzane w MZGK nie są udostępniane osobom trzecim (w tym przedsiębiorstwom) nie zaangażowanym w proces dla których zostały zgromadzone.
   3.6. MZGK nie gromadzi żadnych danych osobowych ponad te, które są niezbędne w celu prawidłowej realizacji procesów (usług) świadczonych przez MZGK oraz nie gromadzi danych osobowych w wymiarze szerszym niż niezbędny.

4. **Zapewnienie bezpieczeństwa systemów informatycznych oznacza utrzymanie takich atrybutów informacji jak:**

·**Poufność**, która oznacza ograniczony i ściśle zdefiniowany krąg osób mających dostęp do informacji.
· **Integralność**, to jest zapewnienie niezmienności postaci informacji (postać oryginalna), za wyjątkiem momentów, kiedy informacja ta jest w sposób legalny modyfikowana.
· **Autentyczność (informacji, nadawcy, adresata)** – oznacza to zgodność tożsamości informacji (nadawcy, adresata) z deklaracją do niej przypisaną.
· **Dostępność** (informacji) dla wszystkich uprawnionych do tego osób.
· **Rozliczalność** – oznaczająca precyzyjne i jednoznaczne powiązanie każdego dostępu do informacji z właściwą uprawnioną osobą, która tego dokonała
· Niezawodność pracy całości systemu a w szczególności aplikacji i urządzeń zawierających, przetwarzających, przesyłających informacje podlegające ochronie.

5. **System zabezpieczeń systemów informatycznych obejmuje:**

· **Bezpieczeństwo fizyczne** (strefy bezpieczeństwa, zamykane pomieszczenia, szafy pancerne itp.).
· **Bezpieczeństwo IT.**
· **Bezpieczeństwo organizacyjno-proceduralne.**

6. W celu zapewnienia ochrony informacji na wymaganym poziomie wykorzystywane są zawsze metody i środki ze wszystkich trzech wymienionych w pkt. 5 obszarów. Oznacza to kompleksowy charakter zabezpieczeń. Wszystkie trzy wymienione obszary są jednakowo ważnymi elementami realizacji polityki bezpieczeństwa informacji.

7. **Szczegółowe zasady postępowania przy przetwarzaniu danych osobowych opisuje dokument** „Instrukcja zarządzania systemem informatycznym MZGK".

§ 5.

WYKAZ BUDYNKÓW I POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ PRZEDSIĘBIORSTWA TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

Numer pokoju.	Nazwa pomieszczenia
PARTER	
1	Kierownik działu sieci wodno - kanalizacyjnej
2	Dział sieci wodno - kanalizacyjnej
3	Dział organizacyjno - administracyjny
4	Kierownik działu organizacyjno - administracyjnego
5	Dział spraw pracowniczych i analiz ekonomicznych
5A	Kierownik działu spraw pracowniczych i analiz ekonomicznych
7	Archiwum
8	Zbyt i rozliczenia
I PIĘTRO	
10	Sekretariat
10A	Prezes Zarządu
10B	Główna Księgowa - Prokurent
10C	Kierownik Biura Zarządu
11	Dyrektor Techniczny
12	Kierownik Składowiska odpadów
13	Księgowość i windykacja
14	JRP – Z-ca Kierownika
15	JRP – Sekcja organizacyjna/archiwum
16	Serwerownia
18	JRP – Sekcja techniczna
21	Kierownik działu ogólnobudowlanego
25	JRP - Kierownik
26	JRP – Sekcja techniczna
27	JRP – Sekcja finansowa
28	JRP – Sekcja techniczna
29	Radca Prawny

§ 6.

WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH.

Lp.	Nazwa zbioru	Oprogramowanie
1	Dane kadrowo – płacowe pracowników	KOMAX
2	Dane teleadresowe oraz PESEL odbiorców usług Przedsiębiorstwa (EWIDENCJA ODBIORCÓW)	TPAdmin
3	dane personalne osób zgłoszonych do ubezpieczenia społecznego w ZUS	Płatnik
4	dane kontrahentów ewidencji księgowej (EWIDENCJA DOSTAWCÓW)	TPAdmin
5	dane kontrahentów do przelewów bankowych	Usługa on-line banku
6	Rejestr korespondencji	Książka korespondencji wychodzącej i przychodzącej, pocztowa książka nadawcza,
7	Rejestr zgłoszeń awarii	Zeszyt
8	Dane teleadresowe dostawców odpadów (EWIDENCJA ODBIORCÓW - SKŁADOWISKO)	Wago-Mag

§ 7

OPIS STRUKTURY ZBIORÓW DANYCH WSKAZUJĄCY ZAWARTOŚĆ POSZCZEGÓLNYCH PÓL INFORMACYJNYCH I POWIĄZANIA MIĘDZY NIMI

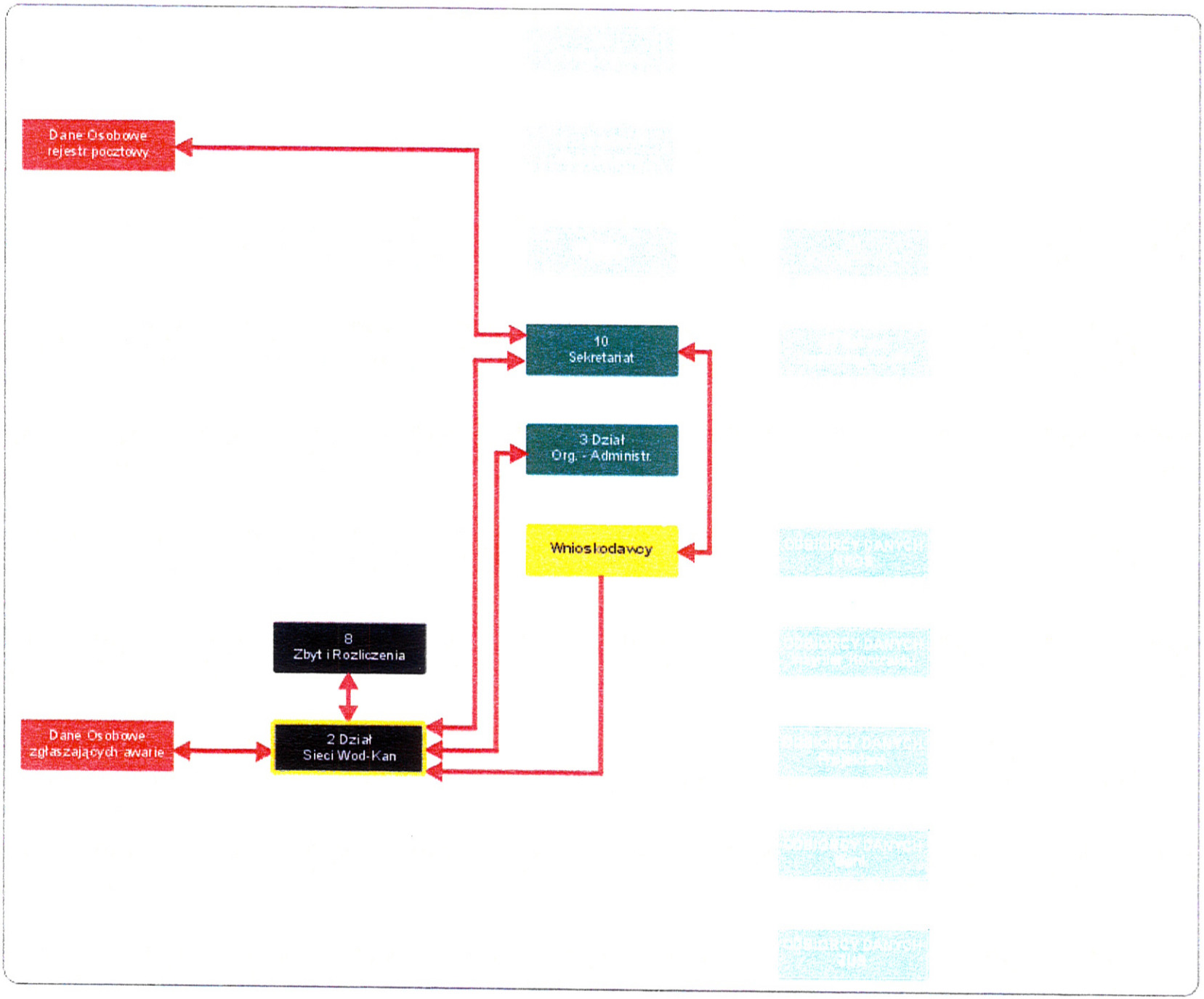
Ze względu na ilość danych dokument ten stanowią pliki na dysku DVD.

Spis zawartości płyty:

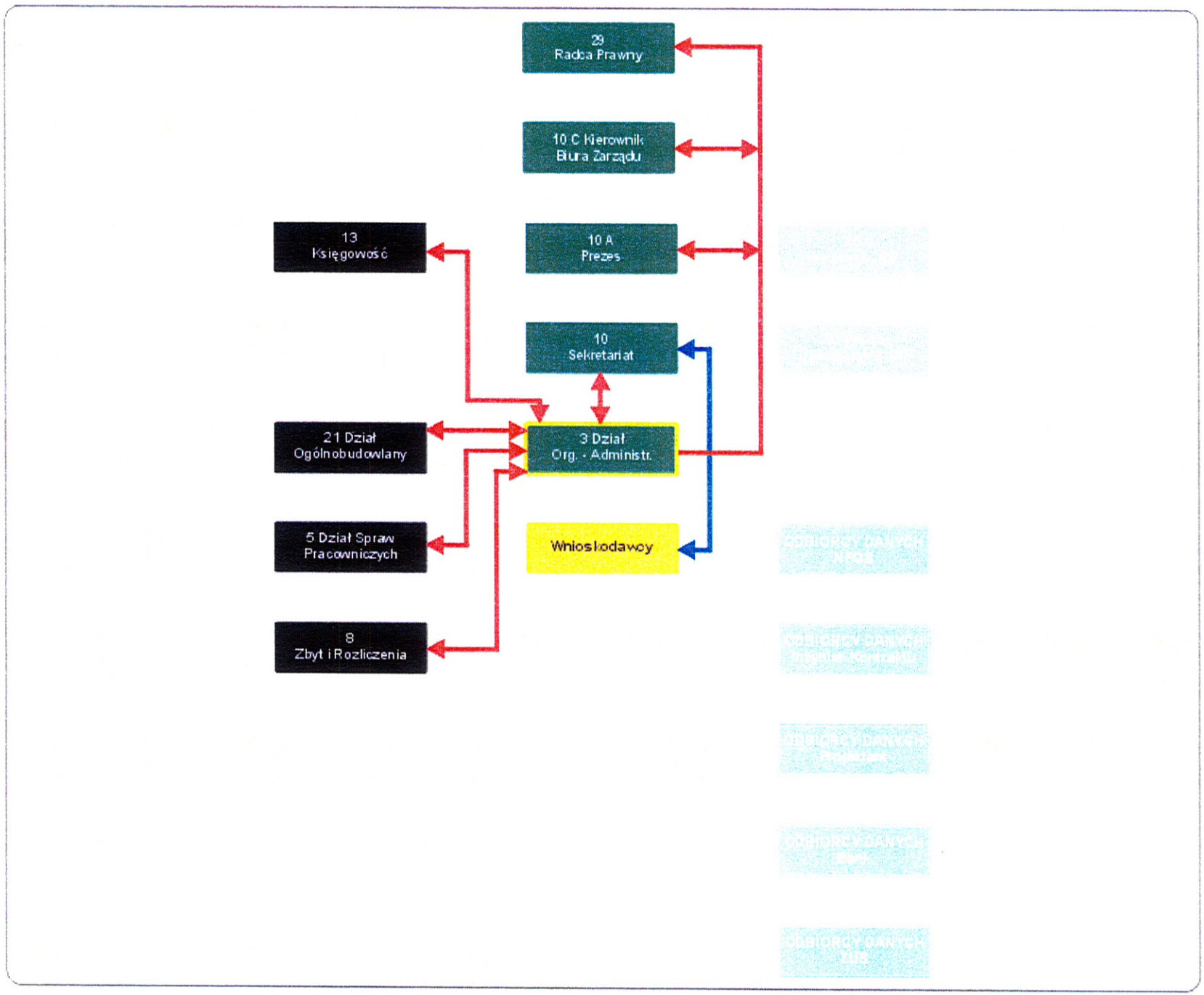
1. Dokumentacja programu Płatnik
2. Dokumentacja programu TPAdmin
3. Dokumentacja programu Komax
4. Dokumentacja programu Wago-Mag
5. Dokumentacja programu BankOnLine

§ 8

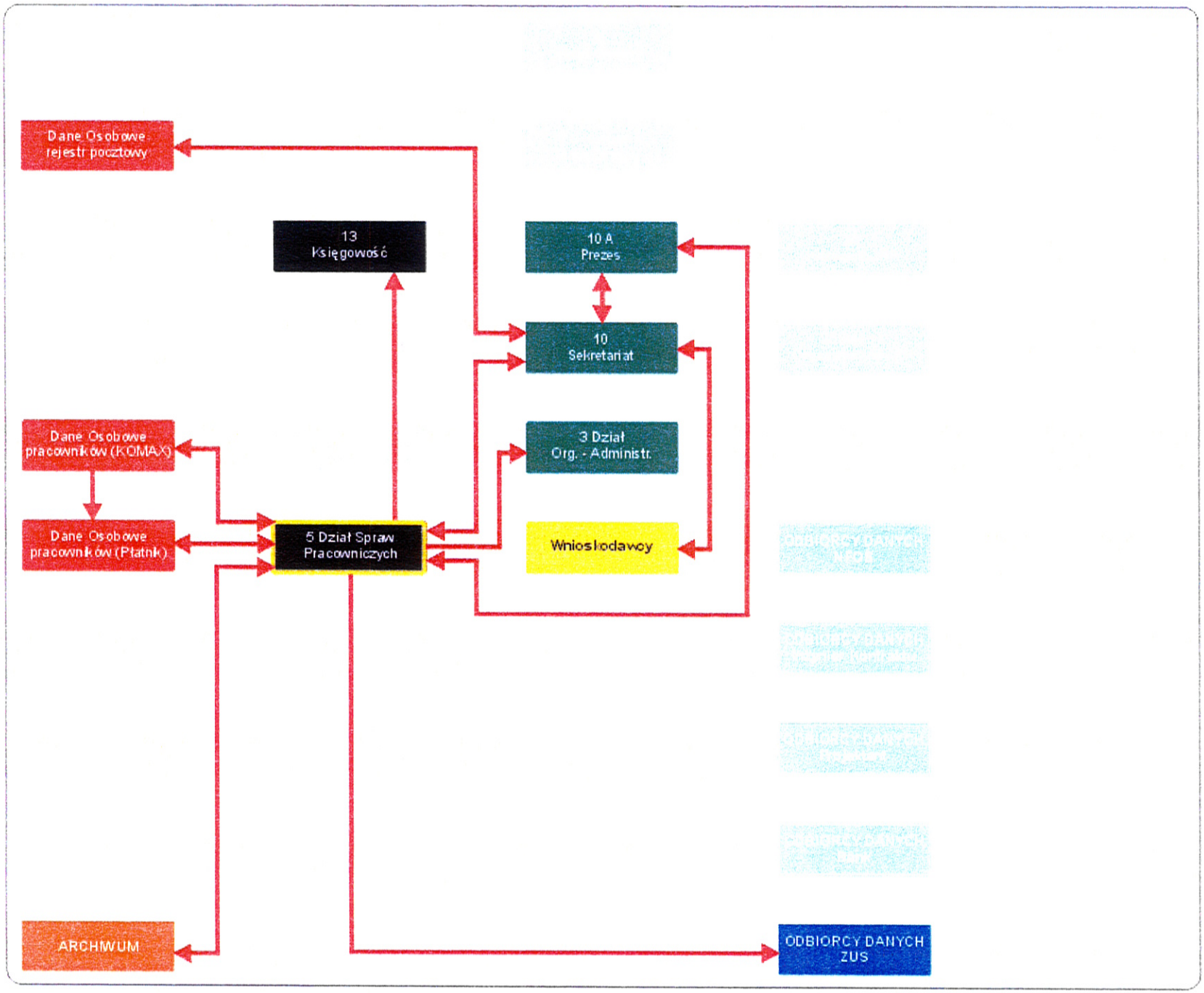
SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI



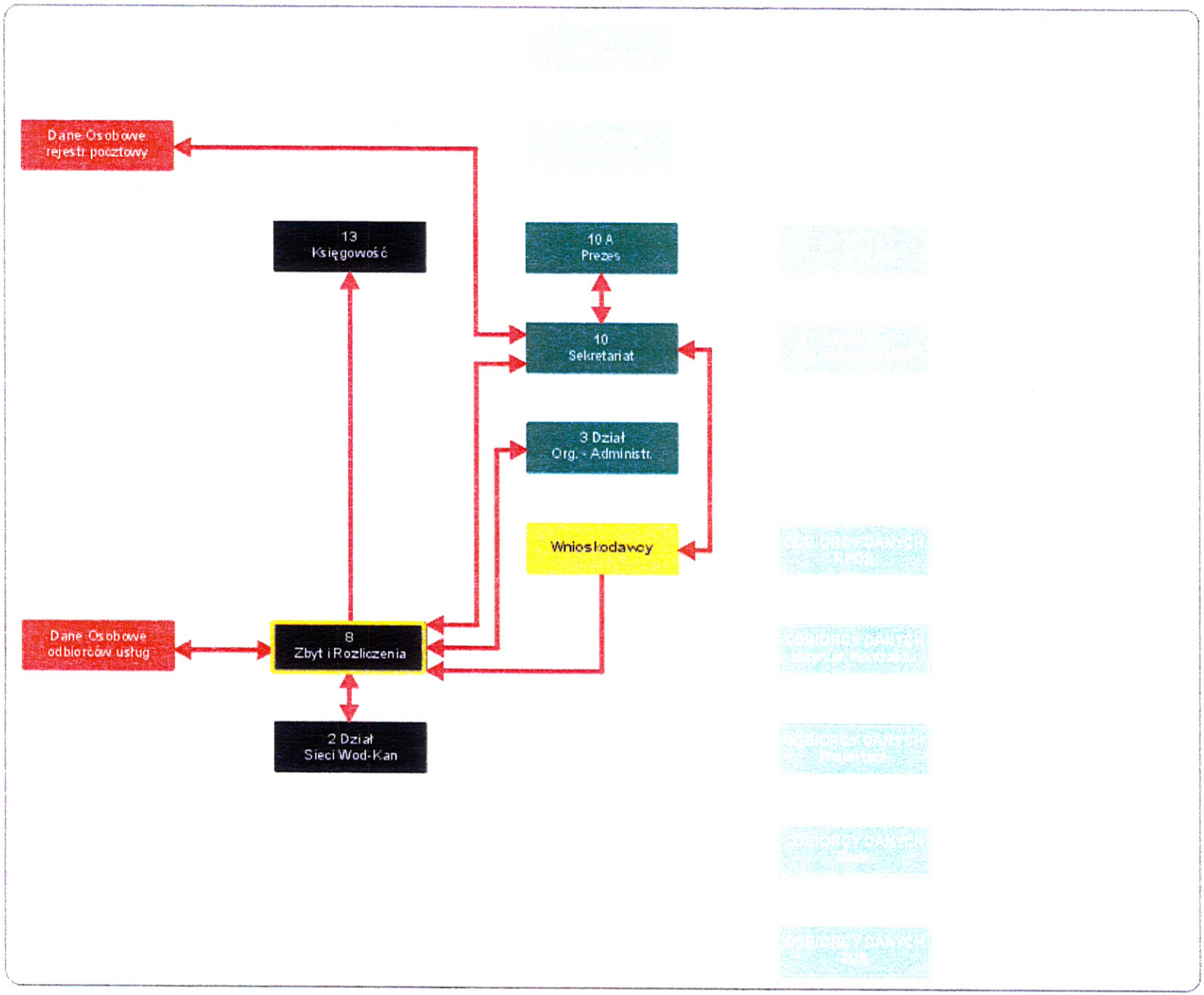
PRZEPŁYWY DANYCH OSOBOWYCH – **DZIAŁ SIECI WODNO - KANALIZACYJNEJ**



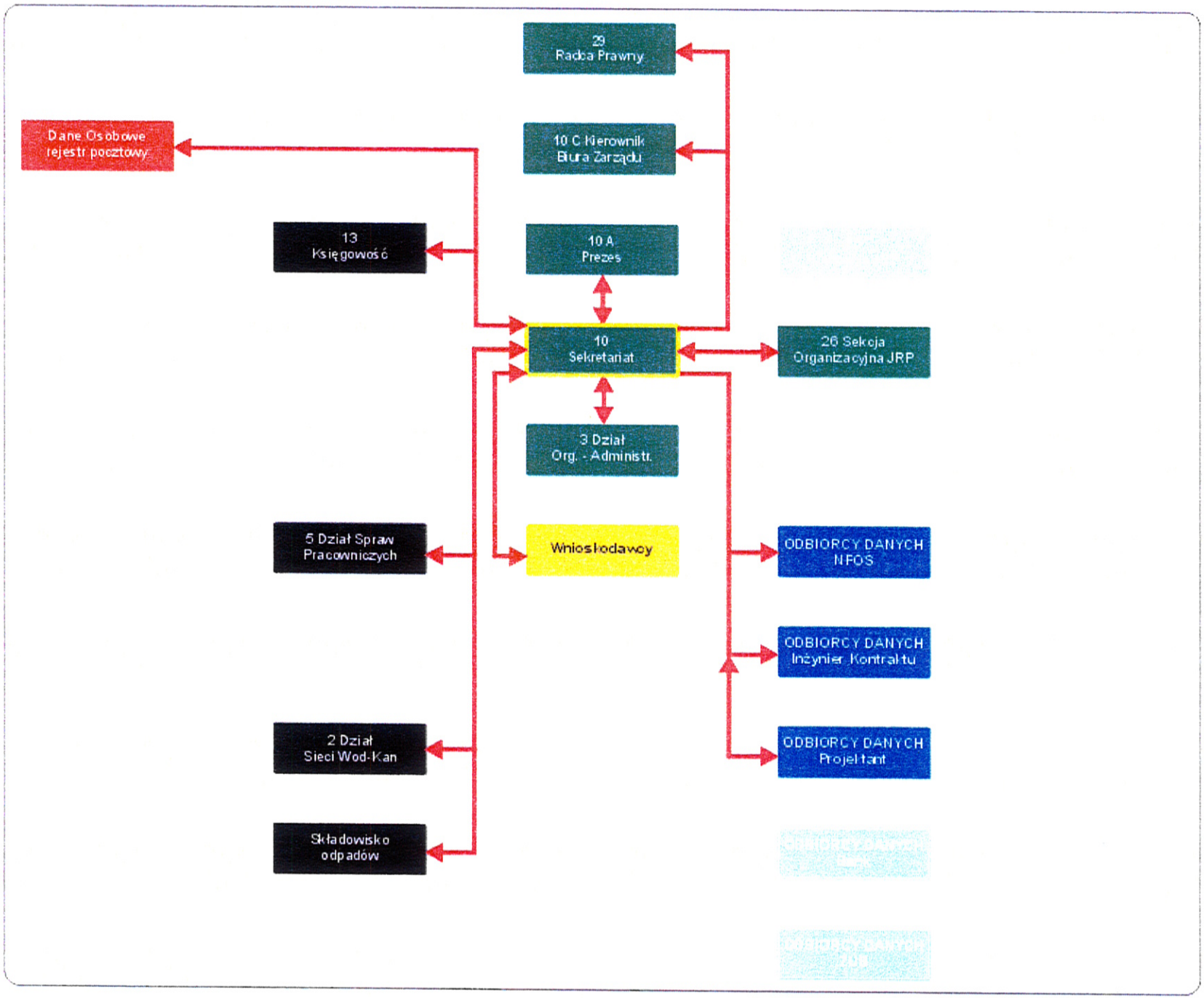
PRZEPŁYWY DANYCH OSOBOWYCH – **DZIAŁ ORGANIZACYJNO - ADMINISTRACYJNY**



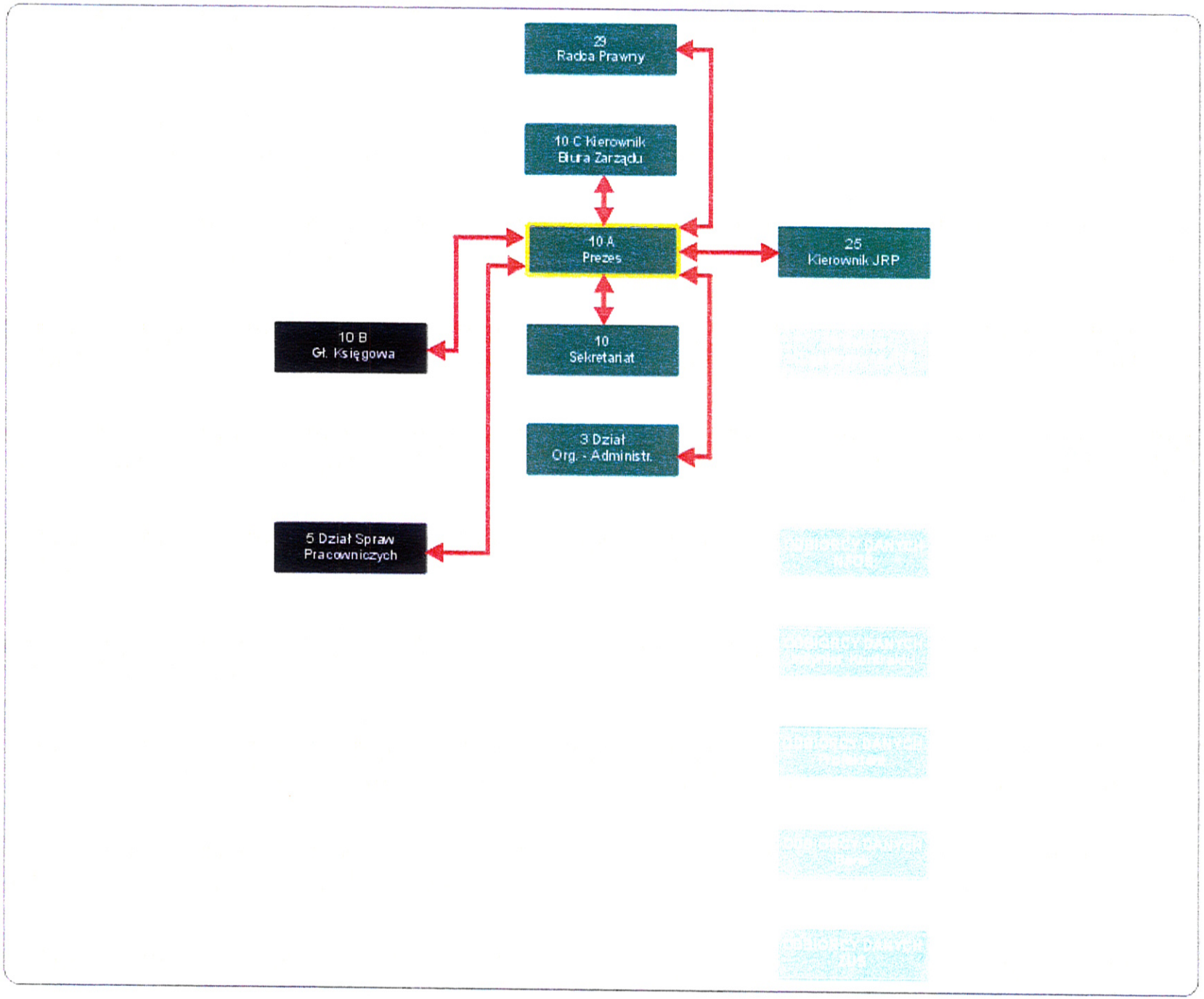
PRZEPŁYWY DANYCH OSOBOWYCH – **DZIAŁ SPRAW PRACOWNICZYCH I ANALIZ EKONOMICZNYCH**



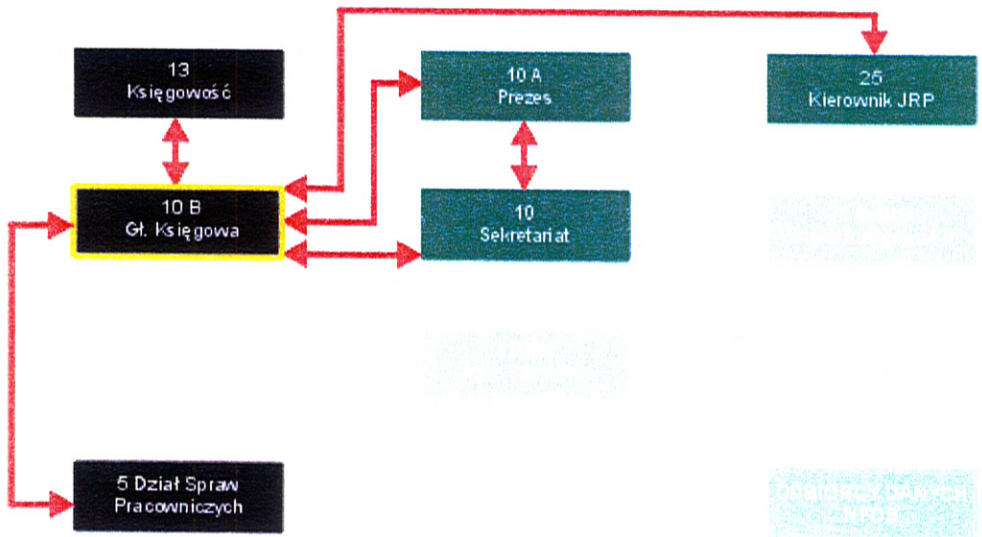
PRZEPŁYWY DANYCH OSOBOWYCH – **ZBYT I ROZLICZENIA**



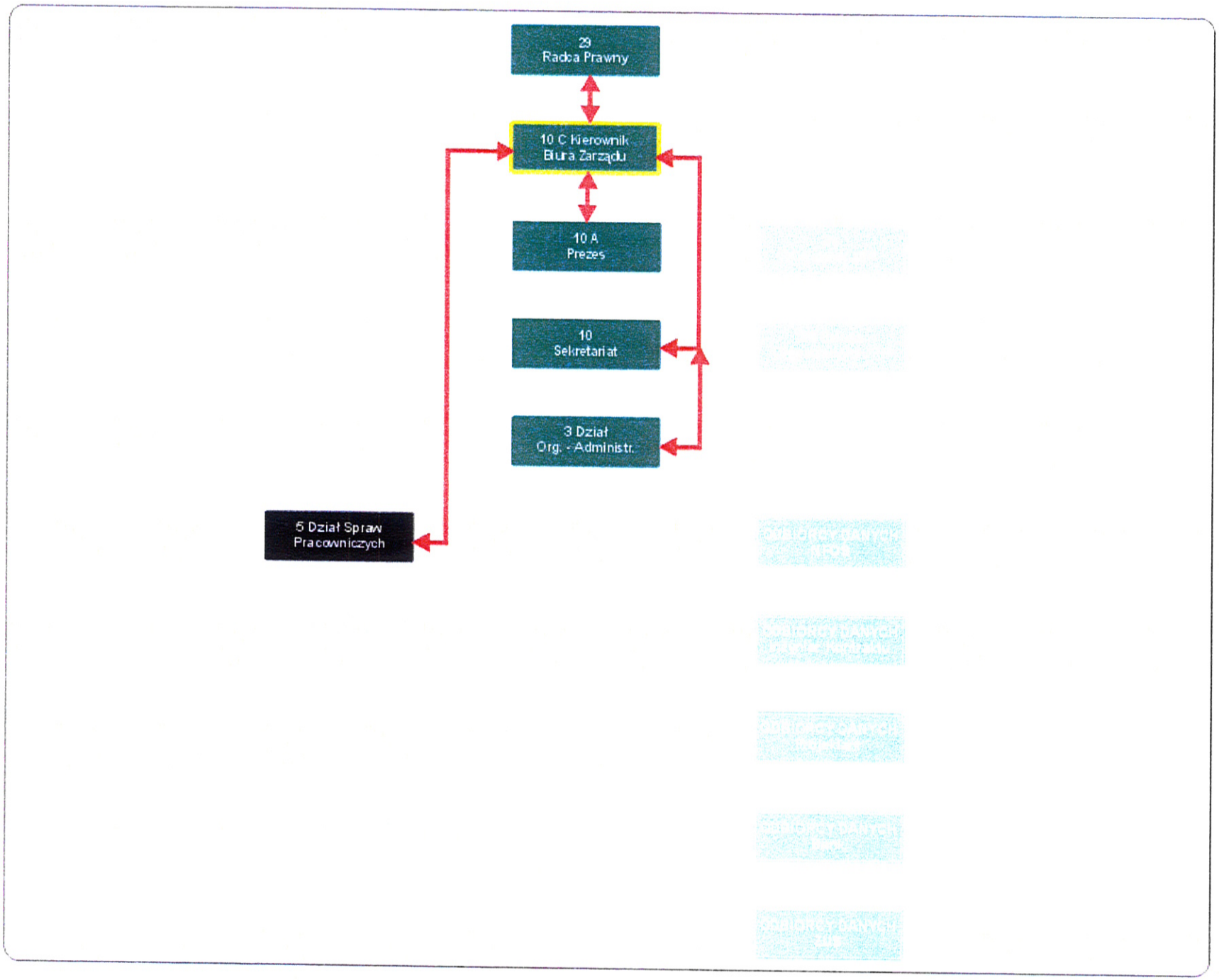
PRZEPŁYWY DANYCH OSOBOWYCH – **SEKRETARIAT**



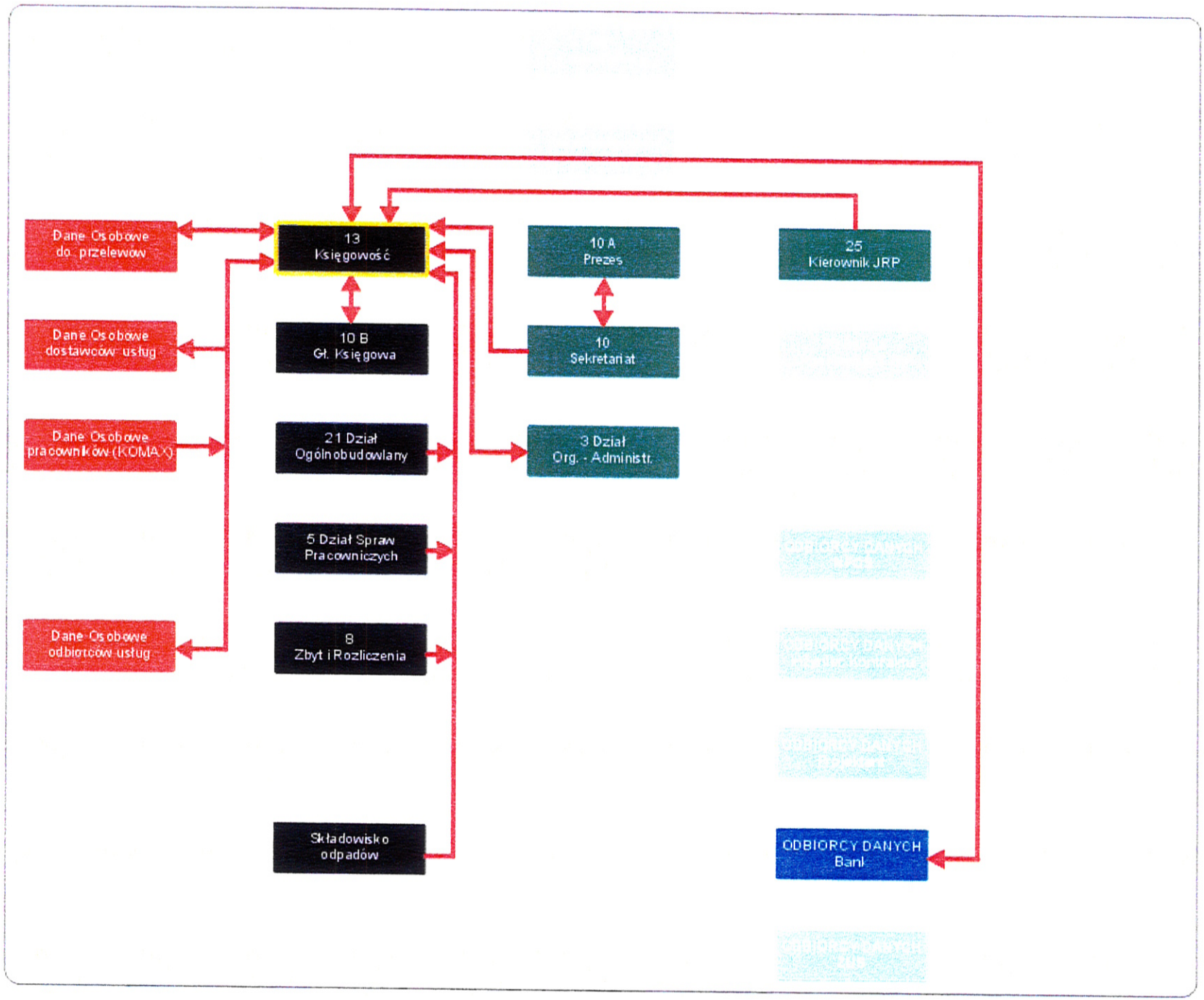
PRZEPŁYWY DANYCH OSOBOWYCH – **PREZES**



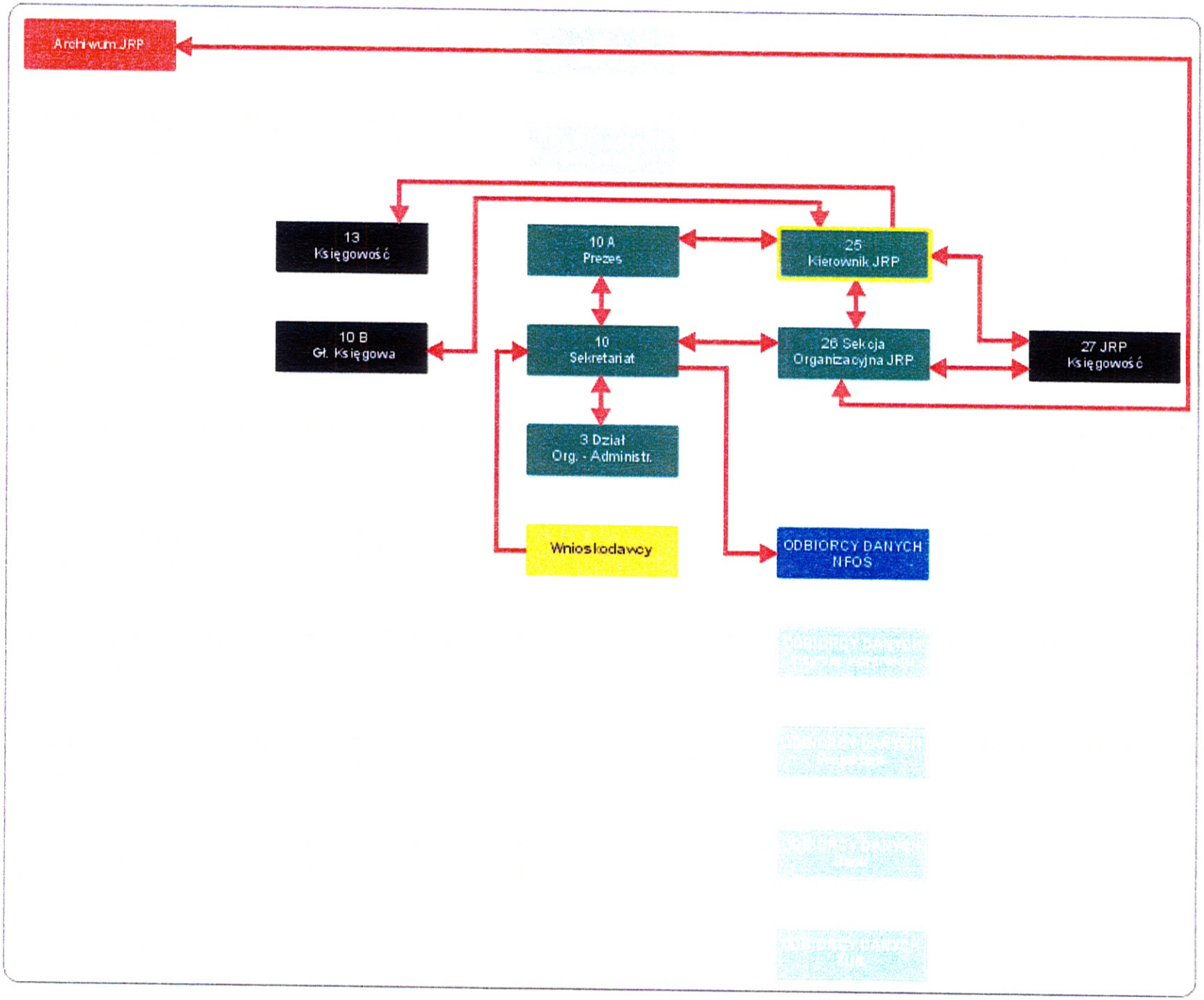
PRZEPŁYWY DANYCH OSOBOWYCH – **GŁÓWNA KSIĘGOWA**



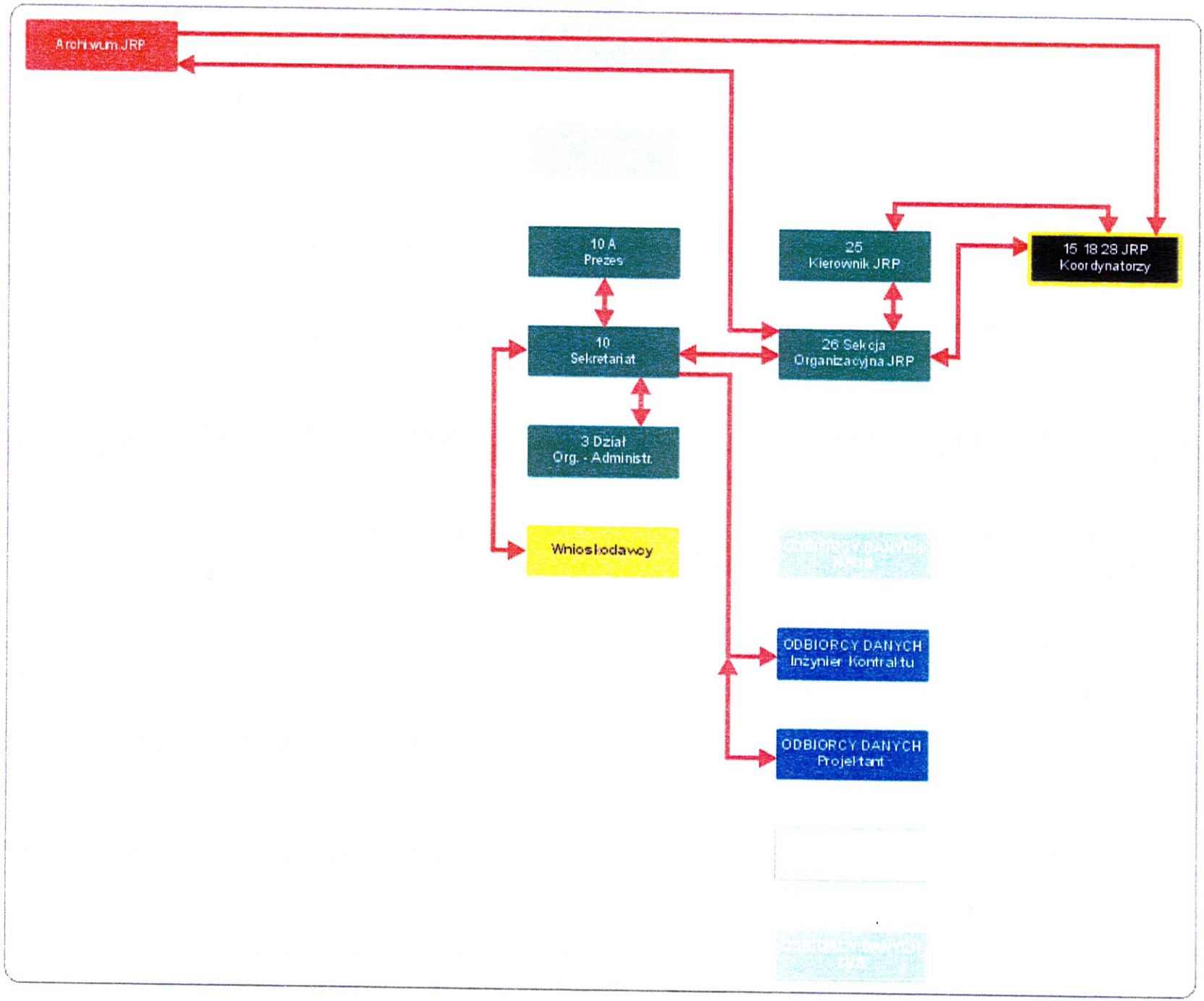
PRZEPŁYWY DANYCH OSOBOWYCH – **KIEROWNIK BIURA ZARZĄDU**



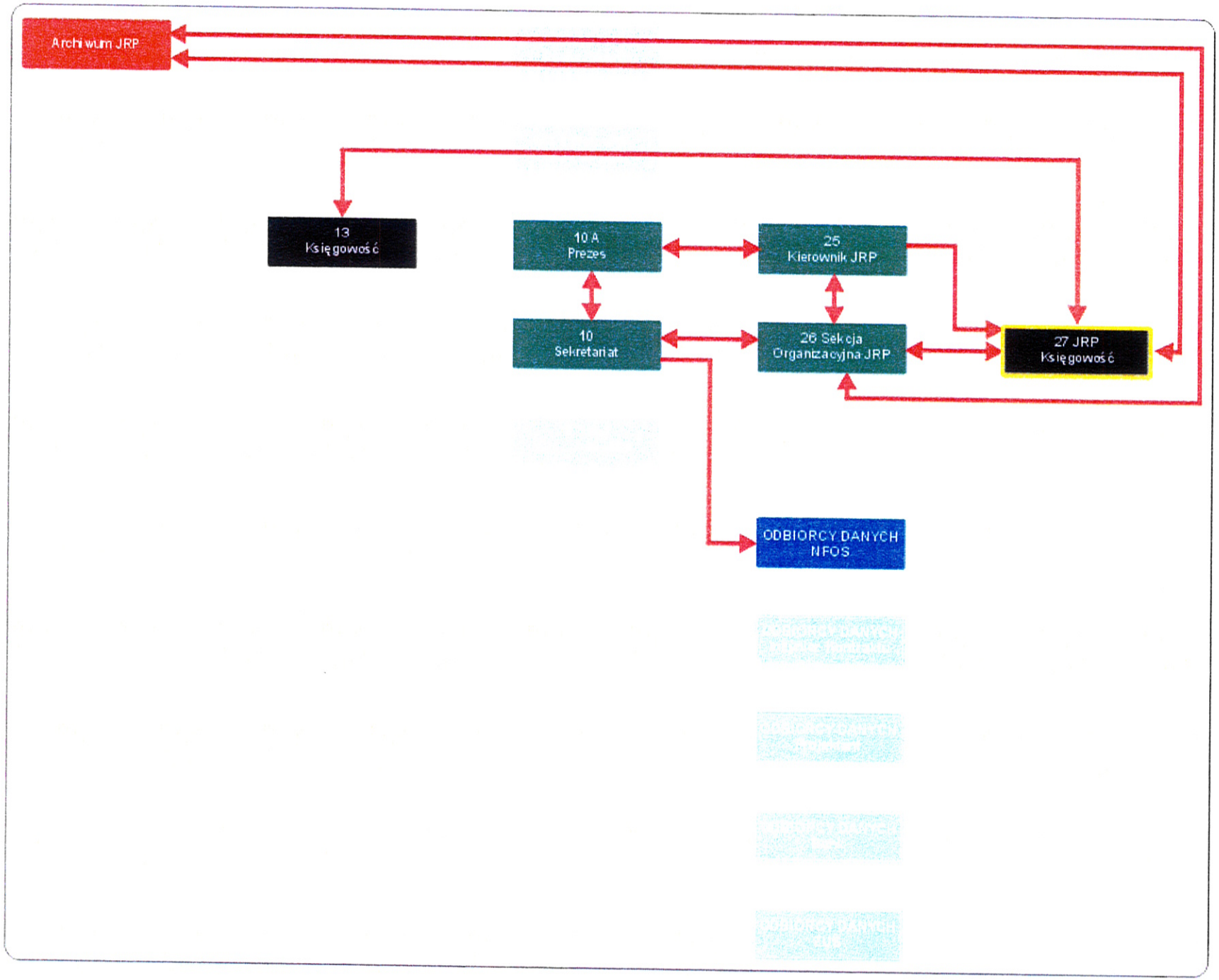
PRZEPŁYWY DANYCH OSOBOWYCH – **KSIĘGOWOŚĆ**



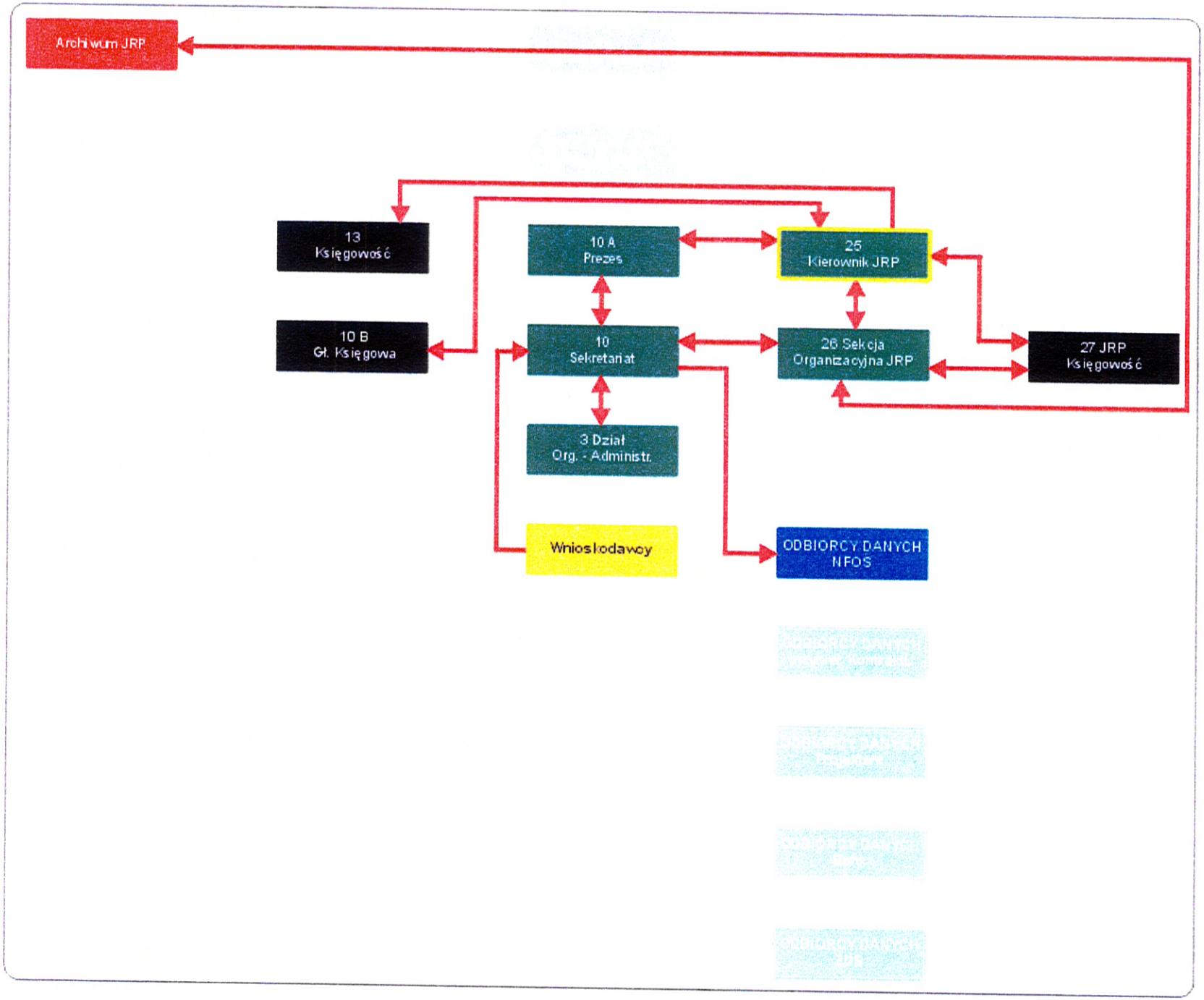
PRZEPŁYWY DANYCH OSOBOWYCH – **JRP: KIEROWNK**



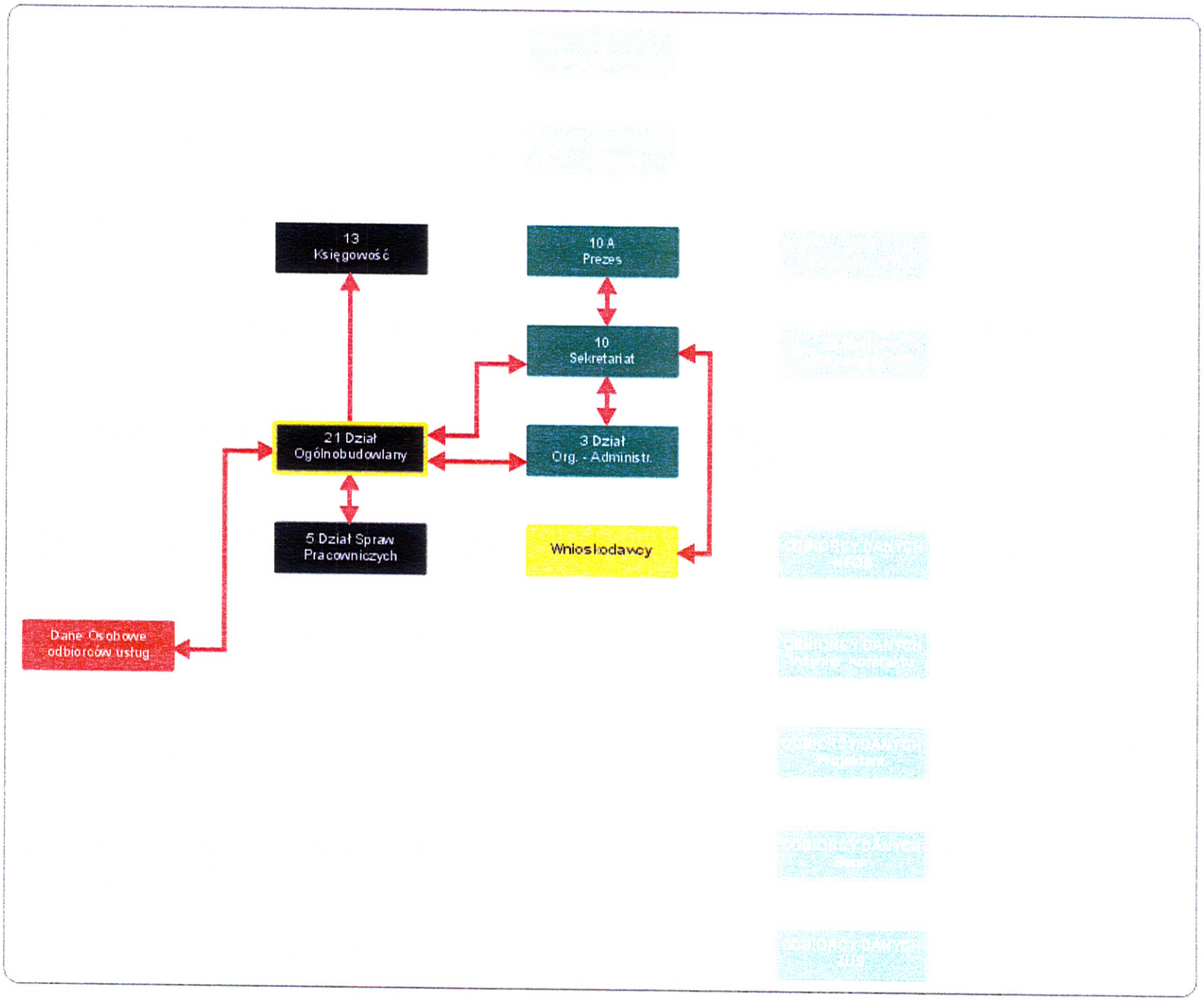
PRZEPŁYWY DANYCH OSOBOWYCH – **JRP: SEKCJE TECHNICZNE**



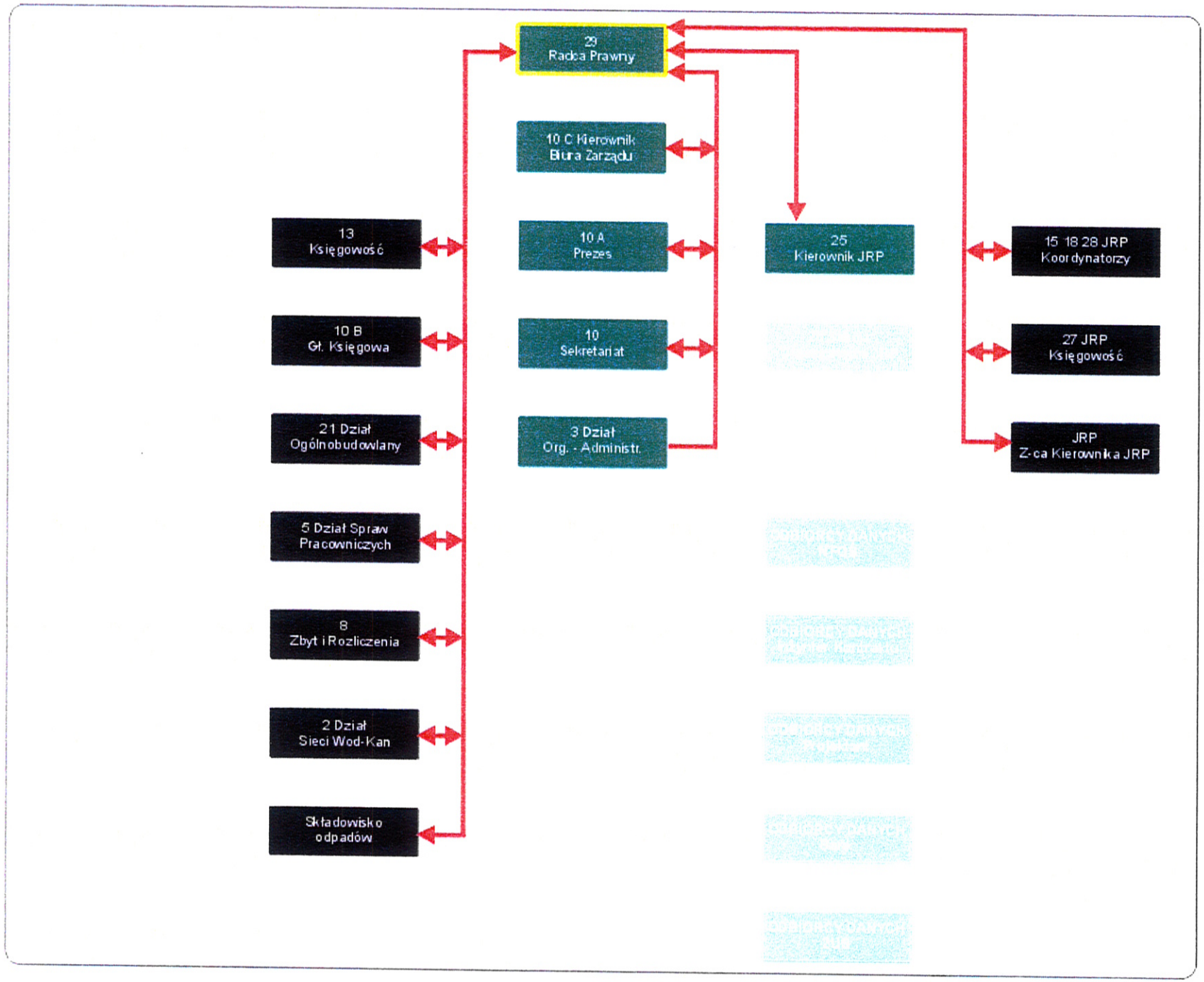
PRZEPŁYWY DANYCH OSOBOWYCH – **JRP: KSIĘGOWOŚĆ**



PRZEPŁYWY DANYCH OSOBOWYCH – **JRP: SEKCJA ORGANIZACYJNA / ARCHIWUM**



PRZEPŁYWY DANYCH OSOBOWYCH – **DZIAŁ OGÓLNOBUDOWLANY**



PRZEPŁYWY DANYCH OSOBOWYCH – **RADCA PRAWNY**

§ 9.

OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DO ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH.

1. **Ochrona budynku Przedsiębiorstwa.**
   1.1. Główne wejście do budynku Przedsiębiorstwa zabezpieczone jest podwójnymi drzwiami. Do budynku można również wejść od strony zaplecza – wejście to zabezpieczone jest drzwiami pojedynczymi. Wszystkie drzwi wejściowe do Przedsiębiorstwa zamykane są na zamki patentowe.
   1.2. Budynek MZGK wyposażony jest w instalację alarmową połączoną z agencją ochrony. System alarmowy należy włączać po godzinach urzędowania i sprzątania niezależnie od obecności pracownika ochrony.
   1.3. Na terenie siedziby głównej przedsiębiorstwa, przez 16h/dobę od 15.00 do 7.00 i 24h/dobę w weekendy, przebywa pracownik ochrony. Przy wejściu głównym do budynku znajduje się przeszkolone pomieszczenie ochrony – jeśli znajduje się w nim pracownik ochrony - każdy wchodzący lub wychodzący musi zostać przez niego zauważony.
   1.4. Zewnętrzny teren Przedsiębiorstwa oraz drzwi wejściowe do budynku głównego są obserwowane przez kamery; obraz z kamer jest nagrywany na dyski HDD.

2. **Ochrona biur i archiwum.**
   2.1. Wszystkie pomieszczenia, w których znajduje się sprzęt komputerowy podłączony do sieci teleinformatycznej, w której przetwarza się dane osobowe, zamykane są na zamek patentowy.
   2.2. Klucze do pomieszczeń znajdują się w pomieszczeniu pracownika ochrony, który zobowiązany jest prowadzić ewidencję używania kluczy.
   2.3. W pomieszczeniu ochrony powinna znajdować się informacja o tym którzy pracownicy mają dostęp do jakich pomieszczeń; pracownik ochrony zobowiązany jest sprawdzać tożsamość osoby, której wydaje klucze jak również czy osoba ta ma ważne uprawnienie dostępu do pomieszczenia.
   2.4. Za aktualność listy praw dostępu, o której mowa w pkt. 2.3 odpowiada Administrator Bezpieczeństwa Informacji. Każdorazowo przy zmianie uprawnień ABI informuje o tym pracownika ochrony, a ten swojego zmiennika tak długo, aż wszyscy zmiennicy zostaną powiadomieni.
   2.5. Osoby, które weszły w posiadanie klucza nie mogą przekazywać go innym osobom, które nie mają do niego uprawnienia.
   2.6. Jeśli pracownik musi wyjść z pomieszczenia powinien wyprosić petenta ; drzwi pomieszczenia należy zamknąć na klucz; nie zostawiać klucza w drzwiach.
   2.7. Podczas pracy w archiwum drzwi powinny być zamknięte. Zabrania się przebywania w archiwum osobom innym niż upoważnione przez Administratora Danych Osobowych zgodnie z zapisami ustawy z dnia 14.07.1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. Nr 97 z 2006 r. poz.673 z póz. zm.) oraz Rozporządzenia Ministra Kultury z dnia 16.09.2002r. (Dz.U. Nr 167/2002 z póz. zm.).

3. **Zabezpieczenie sieci teleinformatycznej.**
   3.1. Ze względu na fakt, że stacje robocze, na których przetwarza się dane osobowe mają połączenie z siecią Internet wprowadza się tzw. **wysoki poziom zabezpieczeń**.
   3.2. Systemy operacyjne komputerów, na których przetwarzane są dane, zabezpieczone są przed nieuprawnionym dostępem wbudowanymi procedurami dostępu do systemu (podanie loginu i hasła).

3.3. Do przechowywania plików danych stosuje się system plików NTFS. Dostęp do plików przyznawany jest przez Administratora Bezpieczeństwa Informacji na podstawie upoważnienia wydanego przez Administratora Danych Osobowych.

3.4. Ruch sieciowy pomiędzy Przedsiębiorstwem a resztą świata odbywa się poprzez firewall, wewnątrz sieć chroniona jest poprzez rozwiązania Microsoft Windows Server.

3.5. W sieci uruchomione jest oprogramowanie antywirusowe oraz chroniące przed innym szkodliwym oprogramowaniem.

3.6. W przedsiębiorstwie powołano 1 osobę odpowiedzialną za system teleinformatyczny, tj. Administratora Systemów i Sieci Komputerowej; osoba ta jest odpowiedzialna za instalację całości oprogramowania dostępnego w systemie. Zabrania się osobom nieupoważnionym instalacji oprogramowania.

3.7. W Przedsiębiorstwie, w Sekretariacie, istnieje Punkt Wymiany Informacji – jedyne miejsce w firmie, w którym dzięki zabezpieczeniom można wymienić pliki z nośników typu pendrive lub płyta CD z obszarem sieci firmowej.

4. Zabezpieczenie sprzętu komputerowego.

4.1. Wszystkie komputery klienckie, serwery oraz aktywny sprzęt sieciowy posiadają własne źródło zasilania awaryjnego pozwalające na sprawne zakończenie pracy oraz automatyczne wyłączenie komputerów i serwerów bez ryzyka utraty danych.

4.2. Ze względu na wysoki poziom bezpieczeństwa danych osobowych ogranicza się dostęp do urządzeń kopiujących, nagrywających itp. (nagrywarki, stacje dyskietek, porty USB).

4.3. Serwery baz danych pracują w zamkniętym, klimatyzowanym pomieszczeniu.

4.4. Należy bezwzględnie przestrzegać czasu pracy urządzeń, określonego przez producenta jako bezpieczny (np. 3 lata dla baterii w zasilaczu UPS, 3 lata dla dysków twardych serwera itp.)

4.5. Wszelkie pliki baz danych przechowywane są wyłącznie na serwerach.

5. Dostęp do danych osobowych.

5.1. Przedsiębiorstwo powinno dążyć do stanu, w którym posiada 1 źródłową bazę danych. Wszelkiego rodzaju dostęp do danych oraz zmiany prowadzone w tej bazie są ewidencjonowane i wykonywane wyłącznie przez osoby upoważnione.

5.2. Wszystkie programy wykorzystywane do przetwarzania danych osobowych powinny posiadać własny system identyfikacji użytkowników oraz rejestry zmian danych osobowych oraz ich udostępniania.

5.3. Poszczególne systemy za pomocą mechanizmu rejestracji powinny zapamiętywać informacje związane z czasem pracy użytkowników. Pracownicy MZGK maja przydzielone zakresy obowiązków zgodnie, z którymi odpowiadają za przetwarzanie określonych baz danych osobowych. W każdym przypadku jest wyznaczona jedna osoba (oraz osoby zastępujące ja na czas nieobecności) odpowiedzialna za konkretny zbiór danych, posiadająca niepowtarzalny identyfikator, który umożliwia rozliczalność wprowadzanych zmian.

5.4. Osoby mające przetwarzać dane osobowe odbywają szkolenie dotyczące ochrony danych osobowych oraz zapoznają się z obowiązującymi w tym zakresie przepisami przed dopuszczeniem do przetwarzania danych osobowych. Pierwsze szkolenie przeprowadzane jest przez ASiS.

5.5. Osoby przetwarzające dane osobowe składają stosowne oświadczenia o zapoznaniu się z przepisami i odpowiedzialnością za naruszenie obowiązujących przepisów oraz zachowaniu tajemnicy także po ustaniu zatrudnienia.

PREZES ZARZĄDU

Waldemar Wrześniak