Uchwała nr O – 06 – II – 2010
Krajowej Rady Izby Architektów
z dnia 24 lutego 2010 roku

w sprawie wprowadzenia polityki bezpieczeństwa przetwarzania danych osobowych w Izbie Architektów RP oraz instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Izbie Architektów RP

Na podstawie art. 33 pkt 14) ustawy z dnia 15 grudnia 2000 r. o samorządach zawodowych architektów, inżynierów budownictwa oraz urbanistów (Dz. U. Z 2001 r., Nr 5, poz. 42, z późn. zm.) w zw. z art. 36 ust. 2 ustawy o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.) oraz z § 3 ust. 1 rozporządzenia 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).

Krajowa Rada Izby Architektów uchwala, co następuje:

§ 1

Niniejszą uchwałą wprowadza się politykę bezpieczeństwa przetwarzania danych osobowych w Izbie Architektów RP oraz instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Izbie Architektów RP – stanowiące odpowiednio załącznik nr 1 i nr 2 do niniejszej uchwały.

§ 2

Wprowadzenie danych do załączników do polityki bezpieczeństwa i do instrukcji zarządzania systemami informatycznymi oraz zmiany i uzupełnienia tych danych nie wymagają zmiany niniejszej uchwały.

§ 3

Uchwała wchodzi w życie z dniem podjęcia, z terminem wdrożenia do końca 2010 r.

Sławomir Żak
Prezes Krajowej Rady

Waldemar Jasiewicz
Sekretarz Krajowej Rady

Uchwałę otrzymują:

1. Minister właściwy ds. budownictwa
2. Okręgowe Rady Izby Architektów

Polityka bezpieczeństwa przetwarzania danych osobowych w Izbie Architektów RP

Rozdział 1
Zasady ogólne

§ 1

1. Polityką bezpieczeństwa objęte są dane osobowe, przetwarzane przez Izbę Architektów RP w formie papierowej oraz z użyciem systemu informatycznego w celu realizacji jej zadań, określonych w ustawie z dnia 15 grudnia 2000 r. o samorządach zawodowych architektów, inżynierów budownictwa oraz urbanistów[1] oraz zadań statutowych i organizacyjnych Izby - w szczególności prowadzenia listy członków Izby oraz nadania uprawnień budowlanych w specjalności architektonicznej bez ograniczeń.
2. Realizacja postanowień niniejszego dokumentu ma zapewnić ochronę danych osobowych, właściwą ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa danych osobowych oraz zapewnić właściwy tryb działania aby właściwie wykonać obowiązki administratora danych w zakresie zabezpieczenia danych osobowych.
3. Przetwarzaniem danych w Izbie Architektów RP w jej imieniu zajmują się jej jednostki organizacyjne: na poziomie okręgowym – okręgowe izby architektów i na poziomie krajowym - Krajowa Izba Architektów.

§ 2

Ilekroć w polityce bezpieczeństwa jest mowa o:

1) danych osobowych należy przez to rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
2) zbiorze danych osobowych należy przez to rozumieć każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
3) przetwarzaniu danych osobowych należy przez to rozumieć wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.
4) administratorze danych osobowych należy przez to rozumieć Izbę Architektów RP.
5) systemie informatycznym należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

[1] Dz. U. z 2001 r., Nr 5, poz. 42 z późn. zm.

6) bezpieczeństwie danych osobowych należy przez to rozumieć wdrożenie środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych przed dostępem, modyfikacją, ujawnieniem, pozyskaniem lub zniszczeniem.
7) użytkowniku systemu należy przez to rozumieć osobę posiadającą uprawnienia do przetwarzania danych osobowych w systemie informatycznym.

§ 3

1. Krajowa Rada Izby Architektów wyznacza krajowego administratora bezpieczeństwa informacji w celu nadzorowania przestrzegania zasad przetwarzania i ochrony danych osobowych w Izbie Architektów RP, zasad ustanowionych w niniejszym dokumencie oraz nadzorowania i koordynowania pracy okręgowych administratorów bezpieczeństwa informacji.
2. Okręgowa rada izby architektów wyznacza okręgowego administratora bezpieczeństwa informacji w celu nadzorowania przestrzegania zasad przetwarzania i ochrony danych osobowych w danej okręgowej izbie architektów.
3. Administrator bezpieczeństwa informacji ma obowiązek ściśle współpracować z administratorem systemu informatycznego w zakresie przetwarzania danych osobowych w systemach informatycznych.

§ 4

1. Krajowy administrator bezpieczeństwa informacji sporządza roczne plany kontroli i zgodnie z nimi przeprowadza kontrole w Krajowej Izbie.
2. Okręgowy administrator bezpieczeństwa informacji sporządza roczne plany kontroli i zgodnie z nimi przeprowadza kontrole w danej okręgowej izbie, oraz przesyła krajowemu administratorowi bezpieczeństwa informacji raport z przeprowadzonej kontroli.
3. Administrator bezpieczeństwa informacji w związku ze stwierdzonymi podczas kontroli nieprawidłowościami w zakresie przestrzegania procedur bezpieczeństwa informacji może wydać wiążące polecenia oraz poinformować bezpośredniego przełożonego użytkownika o stwierdzonym fakcie naruszenia dyscypliny pracy (np. nie wylogowanie się przed opuszczeniem stanowiska pracy, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych ujawnienie osobom nieuprawnionym danych osobowych lub objętych tajemnicą procedur ochrony przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń, itp.).

§ 5

Krajowy i okręgowy administrator bezpieczeństwa informacji sporządza roczne sprawozdanie ze swojej działalności, które przedstawia do zatwierdzenia odpowiednio Krajowej lub okręgowej radzie izby architektów.

§ 6

Krajowa i okręgowe rady izby architektów wyznaczają odpowiednio Krajowego i okręgowego administratora systemu informatycznego, który będzie odpowiedzialny za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do

przetwarzania danych osobowych w danej jednostce organizacyjnej Izby. Do jego obowiązków należy w szczególności:

1) naprawa, konserwacja oraz likwidacja urządzeń komputerowych zawierających dane osobowe,
2) rejestrowanie użytkowników i haseł dostępu w systemie,
3) aktualizowanie oprogramowania systemowego, chyba że aktualizacje wykonywane są automatycznie,
4) aktualizowanie oprogramowania antywirusowego, chyba że aktualizacje wykonywane są automatycznie,
5) okresowe sprawdzanie kopii zapasowych pod kątem ich dalszej przydatności.

Rozdział 2

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

§ 7

Techniczna ochrona danych i ich przetwarzania realizowana jest poprzez wprowadzenie następujących zasad bezpieczeństwa:

1) przetwarzanie danych osobowych może odbywać się wyłącznie w obszarach do tego celu przeznaczonych; wykaz pomieszczeń, w których dopuszczalne jest przetwarzanie danych osobowych stanowi załącznik nr 1 do niniejszej polityki bezpieczeństwa,
2) wszystkie pomieszczenia, w których przetwarza się dane osobowe, są zamykane na klucz w przypadku opuszczenia pomieszczenia przez ostatniego pracownika upoważnionego do przetwarzania danych osobowych – także w godzinach pracy,
3) dane osobowe przechowywane w wersji tradycyjnej (papierowej) lub elektronicznej (np. pendrive, płyta CD/DVD, dyskietka) po zakończeniu pracy są przechowywane w zamykanych na klucz meblach biurowych, a tam, gdzie jest to możliwe – w szafach metalowych lub pancernych, klucze od szafek należy zabezpieczyć przed dostępem osób nieupoważnionych do przetwarzania danych osobowych,
4) nieaktualne lub błędne wydruki zawierające dane osobowe niszczone są w niszczarkach,
5) komputer z dostępem do Internetu musi być zabezpieczony za pomocą oprogramowania antywirusowego oraz anty malware i spyware oraz posiadać oprogramowanie i mechanizmy zabezpieczające przed nieautoryzowanym dostępem z sieci publicznej (firewall),
6) stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej
7) stosuje się odrębne zasilanie sprzętu komputerowego oraz zasilacze awaryjne UPS,
8) stosuje się zasilacze awaryjne UPS w celu ochrony serwerów przed zanikiem zasilania,
9) tworzy się kopie zapasowe zgodnie „Instrukcją zarządzania systemami informatycznymi", z których w przypadku awarii odtwarzane są dane.

§ 8

Organizacyjna ochrona danych i ich przetwarzania realizowana jest poprzez wprowadzenie następujących zasad bezpieczeństwa:

1) dane osobowe przetwarzać może wyłącznie osoba posiadająca pisemne upoważnienie,
2) dostęp do danych osobowych przetwarzanych w systemie informatycznym uzyskuje się wyłącznie po podaniu identyfikatora i właściwego hasła; ich wprowadzenie następuje w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu,
3) identyfikator jest w sposób jednoznaczny przypisany użytkownikowi, użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje lub posługiwał,
4) przebywanie osób nieuprawnionych w pomieszczeniach znajdujących się na obszarze, w którym są przetwarzane dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania,
5) osoby, które zostały upoważnione do przetwarzania danych, są zobowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia, zachowanie tajemnicy obowiązuje zarówno podczas trwania stosunku pracy jak i po jego ustaniu.

Rozdział 3

Zasady postępowania w przypadku naruszenia ochrony danych osobowych

§ 9

1. W przypadku stwierdzenia:
   1) naruszenia lub próby naruszenia integralności systemu lub bazy danych w tym systemie,
   2) awarii sprzętu lub oprogramowania, które wyraźnie wskazuje na umyślne działanie w kierunku naruszenia ochrony danych,
   3) gdy jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazują na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
   4) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
   5) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, kradzież itp.)

   każda osoba zatrudniona przy przetwarzaniu danych osobowych jest zobowiązana do niezwłocznego powiadomienia o tym fakcie odpowiednio krajowego lub okręgowego administratora systemu informatycznego. W razie niemożliwości zawiadomienia administratora systemu lub osoby upoważnionej do jego zastępowania należy powiadomić bezpośredniego przełożonego.
2. Do czasu interwencji ze strony administratora systemu informatycznego należy:
   1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,

2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
3) zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę zdarzenia,
4) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego lub aplikacji użytkowej,
5) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
6) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora bezpieczeństwa informacji.

3. Po uzyskaniu informacji o naruszeniu ochrony danych osobowych, administrator systemu informatycznego lub upoważniona przez niego osoba:
   1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy danej jednostki organizacyjnej Izby Architektów,
   2) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
   3) jeżeli zasoby systemu na to pozwalają, generuje i drukuje wszystkie raporty, które mogą pomoc w ustaleniu wszelkich okoliczności zdarzenia,
   4) podejmuje odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych:
      a) fizycznie odłącza urządzenia i segmenty sieci, które mogłyby umożliwić dostęp do bazy danych osobie niepowołanej,
      b) wylogowuje użytkownika podejrzanego o naruszenie ochrony danych,
      c) zmienia hasła konta administratora i użytkownika, poprzez które uzyskano
   5) nielegalny dostęp w celu uniknięcia ponownej próby uzyskania takiego dostępu
   6) jeżeli zachodzi taka potrzeba powiadamia odpowiednie organy uprawnione do ścigania przestępstw o fakcie celowego naruszenia bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym,
   7) jeżeli naruszenie było spowodowane celowym działaniem, jest on zobowiązany do pisemnego powiadomienia administratora danych osobowych
4. Po wyczerpaniu niezbędnych środków doraźnych, Administrator systemu informatycznego zasięga niezbędnych opinii i proponuje postępowanie naprawcze oraz ustosunkowuje się do kwestii ewentualnego odtworzenia danych z kopii zapasowych i terminu wznowienia przetwarzania danych.
5. Z przeprowadzonej interwencji Administrator systemu informatycznego sporządza raport - zgodnie z wzorem stanowiącym załącznik nr 2 do niniejszej polityki bezpieczeństwa, który przesyła Krajowemu administratorowi bezpieczeństwa informacji.

6. Krajowy administrator bezpieczeństwa informacji odpowiedzialny jest za przeprowadzenie przynajmniej raz w roku analizy zaistniałych naruszeń w celu określenia skuteczności podejmowanych działań wyjaśniających i naprawczych oraz określenia ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

Rozdział 5

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

§ 10

1. Aktualny wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych znajduje się w Instrukcji zarządzania systemami informatycznymi.
2. Instrukcja powinna być aktualizowana po wprowadzeniu do przetwarzania nowych zbiorów danych osobowych lub nowych programów, które je obsługują.

Rozdział 6

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

§ 11

1. Aktualny opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi znajduje się w Załączniku 3 do niniejszego dokumentu.
2. Załącznik powinien być aktualizowany po wprowadzeniu istotnych zmian w strukturze bazy danych, którą opisuje. W przypadku systemów, które są rozbudowywane wprowadzone zmiany rejestruje się (aktualizując odpowiedni załącznik) nie rzadziej niż co 2 miesiące.

Rozdział 7

Sposób przepływu danych pomiędzy poszczególnymi systemami

§ 12

1. Aktualny opis sposobu przepływu danych pomiędzy poszczególnymi systemami znajduje się w Załączniku 4 do niniejszego dokumentu.
2. Załącznik powinien być aktualizowany po wprowadzeniu istotnych zmian w sposobie lub zakresie wymiany danych, którą opisuje. W przypadku systemów, które są rozbudowywane wprowadzone zmiany rejestruje się (aktualizując odpowiedni załącznik) nie rzadziej niż co 2 miesiące.

Rozdział 8

Postanowienia końcowe

§ 13

1. Obowiązkiem osób zatrudnionych przy przetwarzaniu danych osobowych jest przestrzeganie postanowień niniejszej polityki bezpieczeństwa.
2. Przypadki naruszenia obowiązków wynikających z niniejszej polityki bezpieczeństwa, w szczególności przez osobę, która wobec naruszenia ochrony danych osobowych lub

uzasadnionego domniemania takiego naruszenia, nie podjęła działań określonych w niniejszym dokumencie, mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych.

3. W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy:
   1) ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926),
   2) rozporządzenia 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. Nr 100, poz. 1024).

Załącznik nr 1 do Polityki bezpieczeństwa przetwarzania danych osobowych w Izbie Architektów RP

Wykaz pomieszczeń,
w których przetwarzane są dane osobowe w Izbie Architektów

Lp.	Jednostka organizacyjna IA RP	Lokalizacja(adres)	Nr pokoju/ nazwa pomieszczenia	Nazwa zbioru danych
1				

Załącznik nr 2 do Polityki bezpieczeństwa przetwarzania danych osobowych w Izbie Architektów RP

Wzór raportu z naruszenia bezpieczeństwa przetwarzania danych osobowych w Izbie Architektów RP

1. Data: ..... Godzina: .....
2. Osoba powiadamiająca o zaistniałym zdarzeniu:
.....
(imię, nazwisko, stanowisko służbowe, identyfikator Użytkownika (jeśli występuje)
3. Lokalizacja zdarzenia:
.....
(np. nr pokoju, nazwa pomieszczenia)
4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:
.....
.....
.....
.....
5. Podjęte działania:
.....
.....
.....
.....
6. Przyczyny wystąpienia zdarzenia:
.....
.....
.....
.....
7. Postępowanie wyjaśniające:
.....
.....
.....

.....
(czytelny podpis)

Dane osobowe architekta
nrew character(7) NOT NULL DEFAULT ''::bpchar,
tytul character varying(10),
tytul_dop character varying(10),
imiona character varying(50),
nazwisko character varying(100),
nazwisko_panienskie character varying(100),
imiona_ojciec character varying(30),
imiona_matka character varying(30),
obywatelstwo character varying(30),
pesel character varying(13),
nip character varying(14),
regon character varying(20),
miejsce_ur character varying(100),
data_urodzenia timestamp without time zone,
data_zgonu timestamp without time zone,
oia_status character varying(15),
oia_status_data timestamp without time zone,
oia_status_powod character varying(100),
oia_funkcja character varying(100),
oia_data_wpisu timestamp without time zone,
oia_delegat_krajowy smallint,
oia_delegat_okregowy smallint,
oia_delegat_okreg character varying(50),
oia_pieczatka_data timestamp without time zone,
ak_ulica character varying(150),
ak_kodpocztowy character varying(20),
ak_miejscowosc character varying(100),
ak_wojewodztwo character varying(100),
az_ulica character varying(150),
az_kodpocztowy character varying(20),
az_miejscowosc character varying(100),
az_wojewodztwo character varying(100),
tel_praca character varying(100),
tel_kom character varying(100),
tel_dom character varying(100),
tel_inny character varying(100),
email character varying(100),
dyplom_nazwa_uczelni character varying(200),
dyplom_tytul character varying(50),
dyplom_nr character varying(20),
dyplom_data_uz timestamp without time zone,
uprawnienia_nr character varying(50),
uprawnienia_data timestamp without time zone,
uprawnienia_organ character varying(200),
oc_towarzystwo character varying(200),
oc_nr character varying(40),
oc_data_p timestamp without time zone,
oc_data_k timestamp without time zone,
oc_deklaracja_zgody timestamp without time zone,
oc_status character(1),
oc_status_data timestamp without time zone,
oc_dziennik_nr character varying(30),
praca_firma character varying(200),
praca_miejscowosc character varying(100),
praca_kodpocztowy character varying(20),
praca_ulica character varying(200),
praca_stanowisko character varying(200),
nr_kontrahenta character varying(20),

Sposób przepływu danych

Dane przepływają z lokalnych baz danych do centralnej bazy danych w postaci szyfrowanych plików (AES-256).

Przypływ danych jest jednostronny, tzn. Dane przepływają jedynie z Izb Okręgowych do serwera centralnego. Odwrotna komunikacja, czyli zmiana danych osobowych z poziomu serwera, nie jest możliwa.

Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Izbie Architektów RP

Rozdział 1

Zasady ogólne

§ 1

1. Niniejsza instrukcja jest dokumentem regulującym zasady oraz procedury zarządzania i administrowania Systemami Informatycznymi w Izbie Architektów RP. Instrukcja obejmuje swoim zakresem wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w systemach informatycznych Izby Architektów RP:
   1) systemie MDS-MRM wspomagającym pracę Okręgowych Izb Architektów, zainstalowanym w każdej z 16 okręgowych Izb, na co najmniej 1 stanowisku, (dostęp realizowany jest lokalnie lub w lokalnej sieci komputerowej),
   2) systemie MDS-MRM-SERVER wspomagającym pracę Krajowej Rady Izby Architektów, zainstalowany na centralnym serwerze Izby Architektów, (dostęp realizowany jest przez sieć Internet poprzez szyfrowane połączenie SSL).
2. Dane osobowe, których administratorem jest Izba Architektów RP mogą być przetwarzane z użyciem systemu informatycznego tylko na potrzeby realizowania zadań określonych w ustawie z dnia 15 grudnia 2000 r. o samorządach zawodowych architektów, inżynierów budownictwa oraz urbanistów[2] oraz zadań statutowych i organizacyjnych Izby- w szczególności prowadzenia listy członków Izby oraz nadania uprawnień budowlanych w specjalności architektonicznej bez ograniczeń.
3. Przetwarzaniem danych w Izbie Architektów RP w jej imieniu zajmują się jej jednostki organizacyjne: na poziomie okręgowym – okręgowe izby architektów i na poziomie krajowym - Krajowa Izba Architektów.

§ 2

Ilekroć w niniejszej instrukcji jest mowa o:

1) danych osobowych należy przez to rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
2) danych sensytywnych należy przez to rozumieć dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także informacje o innych orzeczeniach wydanych w postępowaniu sądowym lub administracyjnym,

[2] Dz. U. z 2001 r., Nr 5, poz. 42 z późn. zm.

3) zbiorze danych osobowych należy przez to rozumieć każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
4) przetwarzaniu danych osobowych należy przez to rozumieć wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.
5) administratorze danych osobowych należy przez to rozumieć Izbę Architektów RP,
6) systemie informatycznym należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
7) bezpieczeństwie systemu informatycznego należy przez to rozumieć wdrożenie środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych przed dostępem, modyfikacją, ujawnieniem, pozyskaniem lub zniszczeniem,
8) użytkowniku należy przez to rozumieć osobę posiadającą uprawnienia do przetwarzania danych osobowych w systemie informatycznym,
9) osobie uprawnionej należy przez to rozumieć osobę posiadająca upoważnienie wydane przez administratora danych osobowych do wykonywania w jego imieniu określonych czynności,
10) ustawie należy przez to rozumieć ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2002 r., Nr 101, poz.926, z późn. zm.),

Rozdział 2

Nadawanie uprawnień do przetwarzania danych oraz ich rejestrowanie w systemie informatycznym

§ 3

1. Przetwarzanie danych osobowych może dokonywać jedynie osoba upoważniona do tego przez administratora danych osobowych lub osobę uprawnioną. Wzór upoważnienia stanowi Załącznik nr 1 do niniejszej instrukcji.Oryginał upoważnienia zostaje przekazany pracownikowi za potwierdzeniem odbioru, kopiavzostaje dołączona do akt osobowych pracownika oraz przekazana do wiadomości przełożonego pracownika.
2. Każdy użytkownik systemu przed uzyskaniem upoważnienia musi zobowiązać się do zachowania w tajemnicy przetwarzanych danych osobowych oraz zapoznać się z:
   1) przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 Nr 101, poz. 926 z pózn. zm.),
   2) przepisami rozporządzenia 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. Nr 100, poz. 1024).
   3) polityką bezpieczeństwa przetwarzania danych osobowych w Izbie Architektów RP,
   4) niniejszą instrukcją.

Zobowiązanie do zachowania w tajemnicy oraz zapoznanie się z powyższymi informacjami użytkownik potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi załącznik nr 2 do niniejszej instrukcji.

3. Administrator danych osobowych lub osoba uprawniona przed udzieleniem upoważnienia zgłasza do Krajowego administratora systemu informatycznego potrzebę nadania uprawnień w systemie informatycznym na wymaganym poziomie, na formularzu stanowiącym Załącznik nr 3 do niniejszej instrukcji.
4. Krajowy administrator systemu informatycznego na podstawie otrzymanego formularza:
   1) rejestruje użytkownika w systemie i nadaje mu w systemie wymagane uprawnienia lub usuwa jego konto z systemu,
   2) informuje osobę, która przesłała formularz o fakcie nadania/odebrania uprawnień, w przypadku nadania uprawnień, informuje dodatkowo o założonym koncie dla użytkownika (indentyfikator i hasło) i nadanych uprawnieniach.
5. Nadanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora, hasła oraz zakresu dostępnych danych i operacji. Stosowany w Izbie Architektów schemat uprawnień dostępu do systemu informatycznego zakłada, iż użytkownicy uzyskują dostęp do systemu na z góry zdefiniowanym poziomie użytkownika w zależności od zakresu obowiązków i powierzonych zadań do wykonania na danym stanowisku.
6. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych, należy niezwłocznie wyrejestrować z systemu informatycznego, unieważnić jej hasło, oraz podjąć inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych.
7. Przepisy ust. 3-6 stosuje się odpowiednio w przypadku odebrania lub zmiany danych w istniejących uprawnieniach użytkownika.

§ 4

1. Nazwy i hasła użytkowników posiadających uprawnienia administratorów systemów informatycznych powinny być przechowywane w zamkniętej szafie ulokowanej w pomieszczeniach Biura Krajowej lub okręgowej rady izby architerków (odpowiednio), do której dostęp jest w pełni kontrolowany, przy czym dostęp do szafy mają wyłącznie uprawnione osoby. Nazwy użytkowników oraz hasła powinny być przechowywane w opieczętowanej i opatrzonej podpisem administratorów systemu kopercie. W przypadku konieczności awaryjnego użycia nazw i haseł tych użytkowników konieczny jest wpis ilustrujący zaistniała sytuację w „Dzienniku haseł" znajdującym się w szafie wraz z kopertą, w której znajdują się hasła. Wpis powinien zawierać następujące informacje:
   2) imię i nazwisko oraz stanowisko osoby upoważnionej udostępniającej dostęp do szafy, w której znajdują się hasła,
   3) imię i nazwisko oraz stanowisko osoby, która pobiera nazwy użytkowników i hasła,
   4) krótki opis sytuacji, która zmusiła do awaryjnego wykorzystania haseł.

2. O konieczności i okolicznościach awaryjnego użycia nazw i haseł musi niezwłocznie zostać powiadomiony Krajowy lub okręgowy administrator bezpieczeństwa informacji (odpowiednio).

§ 5

1. Okręgowa oraz Krajowa Rada Izby Architektów prowadzą ewidencję użytkowników w danej izbie i są odpowiedzialne za ich aktualizację. Ewidencję prowadzi się zgodnie z wzorem stanowiącym załącznik nr 4 do niniejszej instrukcji.
2. Okręgowe Rady Izby Architektów RP zobowiązane są do przesłania Krajowej Radzie sporządzonej po raz pierwszy ewidencji, a następnie niezwłocznie przesyłać informacje o zmianach w ewidencji.
3. Centralą ewidencję wszystkich użytkowników w Izbie Architektów RP prowadzi Krajowa Rada Izby Architektów. Ewidencję prowadzi się zgodnie z wzorem stanowiącym załącznik nr 4 do niniejszej instrukcji.

Rozdział 3
Metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

§ 6

1. Użytkownik uzyskuje dostęp do danych osobowych przetwarzanych w systemie informatycznym wyłącznie po podaniu identyfikatora użytkownika i właściwego hasła. Użytkownik, po otrzymaniu upoważnienia:
   1) loguje się do systemu w celu sprawdzenia poprawności konta i uprawnień,
   2) przy pierwszym logowaniu się do systemu, użytkownik powinien zmienić nadane mu hasło.
2. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik jest odpowiedzialny za wszystkie czynności wykonane przy użyciu swojego identyfikatora.
3. Identyfikator jest tworzony w następujący sposób: [pierwsza litera imienia][*kropka][nazwisko] i nie zawiera polskich znaków diakrytycznych.
4. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.
5. Użytkownik otrzymuje hasło początkowe przy przystąpieniu do pracy w systemie. Hasło użytkownika powinno mieć minimum 8 znaków, w tym litery i cyfry oraz powinno być zmieniane co 30 dni. Za zmianę hasła odpowiedzialny jest użytkownik. Hasło nie może zawierać żadnych informacji, które można kojarzyć z użytkownikiem komputera np. osobiste dane użytkownika, tj. nazwisko, inicjały, imiona, marka lub nr rejestracyjny samochodu itp. Hasło nie może być zapisywane w miejscu dostępnym dla osób nieuprawnionych.
6. Użytkownik nie może udostępnić swojego identyfikatora oraz hasła jak również dostępu do stanowiska roboczego po uwierzytelnieniu w systemie osobom nieuprawnionym.
7. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie. Hasła wpisywane z klawiatury nie mogą pojawiać się na ekranie monitorów w formie

jawnej. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, użytkownik zobowiązany jest do natychmiastowej zmiany hasła.

8. W przypadku przetwarzania danych na komputerach przenośnych, dyski twarde oraz inne wykorzystywane nośniki informacji mają być zabezpieczone w sposób uniemożliwiający dostęp do tych danych osobom postronnym (np. nieuprawniony dostęp, kradzież komputera, szpiegostwo przemysłowe), poprzez wykorzystanie metod i środków kryptograficznych (szyfrowane partycje dysków twardych, szyfrowanie plików, ochrona fizyczna nośników).

Rozdział 4

Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie

§ 7

1. Rozpoczęcie pracy użytkownika w systemie informatycznym następuje po poprawnym uwierzytelnieniu (zalogowaniu się do systemu).
2. Maksymalna liczna prób wprowadzenia hasła przy logowaniu się do systemu informatycznego wynosi 3. Po przekroczeniu tej ilości prób system blokuje dostęp do zbioru danych na poziomie danego użytkownika. Odblokowania dostępu może dokonać Krajowy lub okręgowy administrator systemu informatycznego (odpowiednio).
3. W przypadku braku aktywności użytkownika na komputerze przez okres dłuższy niż 30 minut następuje automatyczne włączenie wygaszacza ekranu. Wygaszacze ekranu powinny być zaopatrzone w hasła zbudowane analogicznie do haseł używanych przez użytkownika przy logowaniu. Hasło powinno składać się z co najmniej 8 znaków, powinno zawierać małe i wielkie litery oraz cyfry lub znaki specjalne oraz być zmieniane nie rzadziej niż co 30 dni.
4. Użytkownik ma obowiązek wylogowania się z lub wywołania blokowanego hasłem wygaszacza ekranu w przypadku dłuższej, zaplanowanej nieobecności na stanowisku pracy. Stanowisko komputerowe nie może pozostać z uruchomionym i dostępnym systemem bez nadzoru pracującego na nim pracownika.
5. W przypadku zakończenia pracy użytkownik zobowiązany jest wylogować się z systemu, a następnie wyłączyć komputer.
6. Użytkownik niezwłocznie powiadamia Krajowego lub okręgowego administratora systemu informatycznego (odpowiednio) w przypadku braku możliwości zalogowania się na swoje konto.

Rozdział 5

procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

§ 8

1. Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.
2. Kopie zapasowe baz danych wykonywane są:

1) w przypadku Izb Okręgowych automatycznie przez system informatyczny, który je twoorzy i na serwer centralny, kopie zapasowe są następnie zapisywane na streamer. Jest to całościowa kopia zapasowa. Kopia zapasowa nie obejmuje danych zawartych w innych systemach, np. plikach pakietu MS Office.
2) w przypadku serwera centralnego wykonywana jest pełna kopia danych zawartych na serwerze na streamer.

3. Za tworzenie kopii bezpieczeństwa systemu informatycznego odpowiedzialny użytkownik.
4. Kopie zapasowe wykonywane są na płytach CD, DVD, taśmach streamer lub innych elektronicznych nośnikach informacji.

§ 9

1. W przypadku przechowywania kopii zapasowych przez okres dłuższy niż pół roku, wszystkie kopie zapasowe zbiorów danych osobowych oraz aplikacji przetwarzających dane osobowe, których to dotyczy muszą być okresowo (co najmniej raz na pół roku) sprawdzane pod względem ich dalszej przydatności. Czynności te wykonuje administrator systemu informatycznego.
2. Nośniki zawierające kopie zapasowe danych po ich wycofaniu na skutek utraty przydatności lub uszkodzenia podlegają likwidacji.

Rozdział 6
sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

§ 10

1. Elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych, określony w Polityce bezpieczeństwa przetwarzania danych osobowych.
2. Po zakończeniu pracy przez użytkowników systemu, wymienne elektroniczne nośniki informacji są przechowywane w zamykanych szafach biurowych lub kasetkach.

§ 11

1. Kopie zapasowe powinny być przechowywane w innych pomieszczeniach niż te, w których przechowywane są zbiory danych osobowych wykorzystywane na bieżąco. Dostęp do tych pomieszczeń mogą mieć tylko osoby do tego upoważnione.
2. Kopie zapasowe przechowuje się w sposób uniemożliwiający nieuprawnione przejęcie, modyfikacje, uszkodzenie lub zniszczenie.

§ 12

1. W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym.
2. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

§ 13

1. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia sie wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.
2. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymywania danych osobowych pozbawia się wcześniej zapisu tych danych.
3. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do naprawy, pozbawia sie przed naprawa zapisu tych danych albo naprawia sie je pod nadzorem osoby upoważnionej.

Rozdział 7

Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

§ 14

1. W związku z istnieniem zagrożenia dla zbiorów danych osobowych, ze strony wirusów komputerowych oraz tzw. „szkodliwego oprogramowania" typu malware, spyware itp., którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, konieczna jest ochrona sieci komputerowej i stanowisk komputerowych.
2. Wirusy komputerowe oraz wyżej wymienione oprogramowanie mogą pojawić się systemach Izby poprzez: załączniki do poczty elektronicznej, Internet lub elektroniczne nośniki informacji takie jak: dyskietki, płyty CD, DVD, dyski przenośne, pamięci typu flash itp.
3. Komputer z dostępem do Internetu musi być zabezpieczony za pomocą oprogramowania antywirusowego oraz anty malware i spyware oraz posiadać oprogramowanie i mechanizmy zabezpieczające przed nieautoryzowanym dostępem z sieci publicznej (firewall).
4. Użytkownik zobowiązany jest skanowania komputera pod kątem obecności wirusów komputerowych oraz oprogramowania złośliwego – przynamniej 2 razy w tygodniu.
5. Elektroniczne nośniki informacji takie jak dyskietki, dyski przenośne, pamięci typu flash itp. niewiadomego pochodzenia użytkownik powinien każdorazowo sprawdzać programem antywirusowym przed ich użyciem.
6. Przy korzystaniu z poczty elektronicznej należy zwrócić szczególną uwagę na otrzymywane załączniki dołączane do treści wiadomości. Zabrania się otwierania załączników i wiadomości poczty elektronicznej od nieznanych nadawców bez ich uprzedniego sprawdzenia programem antywirusowym.
7. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy użytkownik powinien bezzwłocznie skontaktować się Krajowym lub okręgowym administratorem systemu informatycznego. Administrator systemu informatycznego lub inny wyznaczony pracownik powinien podjąć działania zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:
   1) usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego,

2) odtworzenie plików z kopii zapasowych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane,
3) samodzielną ingerencję w zawartość pliku – w zależności od posiadanych kwalifikacji lub skonsultowanie się z zewnętrznymi ekspertami.

Rozdział 8

Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych

§ 15

1. Na podstawie art. 29 Ustawy udostępnienie danych osobowych może nastąpić w następujących przypadkach:
   1) w celu innym niż włączenie danych do zbioru - administrator danych osobowych lub osoba uprawniona udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa,
   2) dane osobowe, z wyłączeniem danych sensytywnych mogą być także udostępnione w celach innych niż włączenie do zbioru, innym osobom i podmiotom niż wymienione w pkt 1) powyżej, jeżeli w sposób wiarygodny uzasadnią potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą,
2. Dane osobowe udostępnia się na pisemny, umotywowany wniosek. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie.
3. Udostępnione dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

§ 16

1. System informatyczny wykorzystywany do przetwarzania danych osobowych powinien posiadać funkcjonalności umożliwiające odnotowanie informacji o odbiorcach danych z tego systemu .
2. Odbiorcą danych jest każdy, komu udostępnia się dane osobowe, z wyłączeniem:
   1) osoby, której dane dotyczą,
   2) osoby upoważnionej do przetwarzania danych,
   3) przedstawiciela, o którym mowa w art. 31a ustawy,
   4) podmiotu, o którym mowa w art. 31 ustawy,
   5) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,
3. Odnotowanie obejmuje informacje o:
   1) odbiorcy danych,
   2) zakresie udostępnianych danych,
   3) dacie udostępnienia.
4. Obowiązek odnotowania ww. informacji spoczywa na użytkowniku systemu udostępniającemu dane. Odnotowanie informacji powinno nastąpić niezwłocznie po udostępnieniu danych.

Rozdział 9
procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

§ 17

1. Dla zachowania ciągłości pracy i bezpieczeństwa danych przeprowadza się przegląd i konserwację sprzętu komputerowego, systemów oraz nośników informacji służących do przetwarzania danych.
2. Krajowy lub okręgowy administrator systemu informatycznego (odpowiednio) lub osoba przez niego upoważniona dokonuje przeglądów i konserwacji:
   1) nośników informacji służących do przetwarzania danych - w terminach określonych przez producenta sprzętu, a jeśli producent nie przewidział dla danego urządzenia potrzeby dokonywania przeglądów eksploatacyjnych, lub też nie określił ich częstotliwości, to o dokonaniu przeglądu oraz sposobie jego przeprowadzenia decyduje administrator systemu informatycznego,
   2) systemów informatycznych wymienionych w § 1 ust.1 niniejszej Instrukcji - przegląd wykonywany jest po każdej zmianie w oprogramowaniu lub raz w miesiącu i obejmuje sprawdzenie logów systemowych w poszukiwaniu ewentualnych nieprawidłowości, wykonanie istniejących testów jednostkowych, sprawdzenie spójności baz danych.

§ 18

1. Naprawa sprzętu, na którym mogą znajdować się dane osobowe w przypadku, gdy czynności te zleca się osobom nie posiadającym upoważnień do przetwarzania danych powinna odbywać się pod nadzorem osób użytkujących sprzęt, w miejscu jego użytkowania.
2. W przypadku konieczności naprawy poza miejscem użytkowania, w przypadku, gdy czynności te zleca się osobom nie posiadającym upoważnień do przetwarzania danych, sprzęt komputerowy, przed oddaniem do serwisu, powinien być przygotowany zgodnie z §14 ust. 3 instrukcji.

Rozdział 10
Postanowienia końcowe

§ 19

1. Obowiązkiem osób zatrudnionych przy przetwarzaniu danych osobowych jest przestrzeganie postanowień niniejszej instrukcji.
2. W sprawach nie uregulowanych niniejszą instrukcja mają zastosowanie przepisy:
   1) ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (t.j. Dz. U. z 2002 r., Nr 101, poz. 926, późn. zm.),
   2) rozporządzenia 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. Nr 100, poz. 1024).

Wzór upoważnienia do przetwarzania danych osobowych

....., ...

miejscowość data

L.dz. .....

Upoważnienie do przetwarzania danych osobowych

1. Upoważniam Panią/Pana

.....

(imię i nazwisko upoważnianego)

zatrudnioną(-ego) na stanowisku / pełniącą funkcję

.....

w .....

(oznaczenie jednostki organizacyjnej)

do przetwarzania danych osobowych:

……..

……..

……

……

(zakres upoważnienia: wskazanie kategorii danych, które może przetwarzać określona w upoważnieniu osoba lub rodzaj czynności jakich może dokonywać na danych osobowych)

2. Identyfikator (w systemie informatycznym)

……..……..

3. Data nadania upoważnienia oraz data ustania upoważnienia (jeśli jest oznaczona): .....

……

(podpis osoby udzielającej upoważnienia)

……, dnia .....

OŚWIADCZENIE

Oświadczam, ze w związku z przetwarzaniem danych osobowych wynikających z wykonywanych przeze mnie czynności służbowych zapoznałem(am) się z:

1) przepisami ustawy z dnia 29.08.1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2002 r., Nr 101, poz. 926, późn. zm.),
2) przepisami rozporządzenia 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).
3) polityką bezpieczeństwa przetwarzania danych osobowych w Izbie Architektów RP,
4) instrukcją zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Izbie Architektów RP.

Jednocześnie zobowiązuję się zachować w tajemnicy wszelkie dane osobowe przetwarzane w Izbie Architektów RP, z którym zapoznam się w związku lub przy okazji wykonywanych przeze mnie czynności służbowych, a w szczególności nie będę:

a) ujawniać przetwarzanych danych i udostępniać ich osobom nieupoważnionym,

b) ujawniać szczegółów technologicznych używanych w Izbie Achitektów RP systemów oraz oprogramowania.

Niniejsze zobowiązanie obowiązuje również po ustaniu zatrudnienia.

.

.....

czytelny podpis

Składającego Oświadczenie

Załącznik nr 3 do Instrukcji Zarządzania Systemami Informatycznymi w Izbie Architektów RP

Wniosek o nadanie uprawnień dla użytkownika w systemie informatycznym

Nowy użytkownik	Modyfikacja uprawnień	Odebranie uprawnień w systemie

DOTYCZY SYSTEMU: ……

(nazwa aplikacji (bazy danych), w której przetwarzane są dane osobowe)

Imię i nazwisko użytkownika:	**Krajowa/okręgowa izba architektów**
zakres upoważnienia: wskazanie kategorii danych, które może przetwarzać określona w upoważnieniu osoba lub rodzaj czynności jakich może dokonywać na danych osobowych	
Data zagłoszenia:	Wnioskodawca:

……

Podpis wnioskodawcy

Wyżej przedstawiony wniosek wypełnia administrator danych osobowych lub osoba uprawniona.

Załącznik nr 4 do Instrukcji Zarządzania Systemami Informatycznymi w Izbie Architektów RP

Wzór rejestru osób upoważnionych do przetwarzania danych osobowych w Izbie Architektów RP

Lp.	Nazwisko i imię	Nazwa identyfikatora	Stanowisko/funkcja	Zakres upoważnienia	Data nadania upoważ-nienia	Data ustania upoważ-nienia