

ZARZĄDZENIE Nr 9 DYREKTORA GENERALNEGO SŁUŻBY ZAGRANICZNEJ

z dnia 9 maja 2011 r.

w sprawie wdrożenia i eksploatacji Paszportowego Systemu Obsługi Obywatela w Ministerstwie Spraw Zagranicznych i placówkach zagranicznych

Na podstawie art. 25 ust. 4 pkt 1 w związku z ust. 10 ustawy z dnia 21 listopada 2008 r. o służbie cywilnej (Dz. U. Nr 227, poz. 1505 oraz z 2009 r. Nr 157, poz. 1241 i Nr 219, poz. 1706) zarządza się, co następuje:

Przepisy ogólne**§ 1**

Zarządzenie określa:

- 1) zasady eksploatacji oraz administrowania Paszportowym Systemem Obsługi Obywatela, zwanego dalej „PS2O”, w Ministerstwie Spraw Zagranicznych oraz w placówkach zagranicznych;
- 2) zadania komórek organizacyjnych Ministerstwa Spraw Zagranicznych i placówek zagranicznych oraz obowiązki zatrudnionych w nich pracowników związane z wdrożeniem, utrzymaniem, użytkowaniem i zarządzaniem PS2O.

§ 2

Pojęcia używane w zarządzeniu są zgodne z definicjami zawartymi w słowniku obowiązujących pojęć dla potrzeb Księgi Norm Teleinformatycznych i Teletechnicznych, ustalonym w odrębnym trybie.

§ 3

1. Wprowadza się do eksploatacji Paszportowy System Obsługi Obywatela w Ministerstwie Spraw Zagranicznych i placówkach zagranicznych.
2. Dyrektor komórki organizacyjnej Ministerstwa Spraw Zagranicznych właściwej w sprawach teleinformatyki, w porozumieniu z dyrektorem komórki organizacyjnej właściwej w sprawach konsularnych, jest upoważniony do wydania i aktualizowania instrukcji, wytycznych i poleceń określających szczegółowe zasady wdrażania, konfiguracji, eksploatacji technicznej, zarządzania PS2O oraz jego wykorzystania do realizacji zadań służbowych.
3. Użytkownicy i administratorzy ponoszą odpowiedzialność służbową za przestrzeganie zasad użytkowania PS2O określonych w instrukcjach, wytycznych i poleceniach, o których mowa w ust. 2.

Paszportowy System Obsługi Obywatela**§ 4**

1. PS2O służy do informatycznego wsparcia procesów paszportowych oraz do elektronicznej wymiany informacji z instytucjami krajowymi w ramach obowiązujących procedur.

2. PS2O jest eksploatowany w Ministerstwie Spraw Zagranicznych oraz placówkach zagranicznych i stanowi element ogólnokrajowego Paszportowego Systemu Informacyjnego nadzorowanego przez ministra właściwego do spraw wewnętrznych.

3. PS2O składa się z następujących modułów:

- 1) PS2O Konsulat Zagraniczny (PS2O_KZ) — dla użytkowników w placówce zagranicznej;
- 2) PS2O Konsulat Wirtualny (PS2O_KW) — dla użytkowników i administratorów w Ministerstwie Spraw Zagranicznych ;
- 3) PS2O_Paszporty Dyplomatyczne i Paszporty Służbowe (PS2O_PDPS) — dla użytkowników wykonujących zadania z zakresu wydawania paszportów dyplomatycznych oraz paszportów służbowych Ministerstwa Spraw Zagranicznych.

4. PS2O_KZ posiada środowiska: produkcyjne i szkoleniowe.

5. Moduły PS2O_KZ oraz PS2O_KW są utrzymywane, administrowane i rozwijane na zasadach określonych w niniejszym zarządzeniu, natomiast moduł PS2O_PDPS jest utrzymywany, administrowany i rozwijany przez komórkę organizacyjną urzędu obsługującego ministra właściwego do spraw wewnętrznych.

Współpraca PS2O z systemami zewnętrznymi**§ 5**

1. PS2O współpracuje w zakresie wymiany danych z systemami zewnętrznymi wymienionymi w instrukcji, o której mowa w § 3 ust. 2.
2. Współpracę PS2O z systemami zewnętrznymi nadzoruje Administrator systemu.

Zadania komórek organizacyjnych i placówek zagranicznych**§ 6**

1. Dyrektor komórki organizacyjnej Ministerstwa Spraw Zagranicznych właściwej w sprawach konsularnych:
 - 1) wykonuje obowiązki Administratora Danych przetwarzanych w systemie PS2O_KZ i PS2O_KW;
 - 2) współpracuje z komórkami organizacyjnymi urzędu obsługującego ministra właściwego do spraw wewnętrznych w celu zapewnienia zgodności PS2O z obowiązującym prawem;
 - 3) w porozumieniu z komórkami organizacyjnymi urzędu obsługującego ministra właściwego do spraw wewnętrznych i jednostkami budżeto-

- wymi nadzorowanymi przez ministra właściwego do spraw wewnętrznych wyraża zgodę na dopuszczenie systemu zewnętrznego do współpracy z PS2O;
- 4) uczestniczy, we współpracy z Administratorem systemu, w testach PS2O prowadzonych przez komórki organizacyjne urzędu obsługującego ministra właściwego do spraw wewnętrznych oraz jednostki budżetowe nadzorowane przez ministra właściwego do spraw wewnętrznych;
 - 5) we współpracy z komórkami organizacyjnymi urzędu obsługującego ministra właściwego do spraw wewnętrznych i jednostkami budżetowymi nadzorowanymi przez ministra właściwego do spraw wewnętrznych wyposaża użytkowników w karty dostępowe;
 - 6) zapewnia wsparcie merytoryczne dla użytkowników PS2O;
 - 7) przy współpracy z komórką organizacyjną właściwą w sprawach szkoleń definiuje potrzeby oraz zapewnia instruktorów do prowadzenia szkoleń użytkowników w zakresie obsługi PS2O;
 - 8) definiuje i wnioskuje do kierownika placówki zagranicznej o przeprowadzenie zmian organizacyjnych w placówkach zagranicznych wynikających z wdrożenia PS2O;
 - 9) wykonuje inne obowiązki Administratora Danych wskazane w „Polityce Bezpieczeństwa Danych Osobowych” oraz „Instrukcji zarządzania systemami informatycznymi”.
2. Dyrektor komórki organizacyjnej właściwej w sprawach osobowych:
- 1) wykonuje obowiązki Administratora Danych przetwarzanych w systemie PS2O_PDPS;
 - 2) wnioskuje do komórki organizacyjnej urzędu obsługującego ministra właściwego do spraw wewnętrznych o założenie lub usunięcie konta oraz wydanie karty dostępowej do systemu PS2O PDPS;
 - 3) określa funkcje i liczbę stanowisk pracy użytkowników PS2O PDPS zaangażowanych w procedurę wydawania paszportów dyplomatycznych i służbowych MSZ;
 - 4) wykonuje inne obowiązki Administratora Danych wskazane w „Polityce Bezpieczeństwa Danych Osobowych” oraz „Instrukcji zarządzania systemami informatycznymi”.
3. Dyrektor komórki organizacyjnej właściwej w sprawach teleinformatyki:
- 1) pełni funkcję organizatora PS2O w Ministerstwie Spraw Zagranicznych i w placówkach zagranicznych;
 - 2) wyznacza Administratora systemu oraz Administratora pomocniczego;
 - 3) sprawuje nadzór nad wykonywaniem obowiązków przez Administratora systemu, Administratora pomocniczego, Administratorów systemów wspierających, Regionalnych Administratorów Systemów Teleinformatycznych oraz Centrum Wsparcia Technicznego;
 - 4) odpowiada za organizację wdrożeń PS2O, z wyłączeniem szkoleń użytkowników, w tym zapewnia sprzęt i oprogramowanie oraz odpowiada za jego instalację i włączenie do środowiska produkcyjnego;
 - 5) odpowiada za planowanie środków finansowych na funkcjonowanie i rozwój PS2O, w szczególności środków przeznaczonych na jego eksploatację i modyfikację oraz zakup sprzętu i oprogramowania;
 - 6) współpracuje z dyrektorem komórki organizacyjnej właściwej w sprawach konsularnych w celu określenia właściwego sposobu wykorzystywania PS2O a także w zakresie modyfikacji istniejących oraz wprowadzania nowych funkcjonalności.
 - 7) wykonuje inne obowiązki Administratora Bezpieczeństwa Systemu Informatycznego wskazane w „Polityce Bezpieczeństwa Danych Osobowych” oraz „Instrukcji zarządzania systemami informatycznymi”.

Obowiązki Administratora systemu

§ 7

Administrator systemu jest obowiązany:

- 1) wykonywać obowiązki określone w instrukcji, o której mowa w § 3 ust. 2;
- 2) nadzorować prawidłowe funkcjonowanie wszystkich komponentów PS2O a w przypadku wykrycia nieprawidłowości niezwłocznie przystąpić do działań mających na celu przywrócenie jego poprawnej pracy;
- 3) zapewniać ciągłość działania PS2O;
- 4) dokonywać koniecznych zmian konfiguracyjnych PS2O;
- 5) zarządzać i aktualizować PS2O;
- 6) administrować kontami użytkowników i ich uprawnieniami określonymi na podstawie wniosku kierownika placówki dyrektora właściwej w sprawach konsularnych;
- 7) powiadomić Administratora Bezpieczeństwa Informacji oraz Administratora Bezpieczeństwa Systemu Informatycznego o przypadkach wystąpienia ryzyka naruszenia zasad ochrony danych osobowych przetwarzanych w systemie PS2O zgodnie z „Instrukcją postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych”;
- 8) opracować i aktualizować dokumentację techniczną PS2O_KW oraz przedkładać ją do zatwierdzenia dyrektorowi komórki organizacyjnej właściwej w sprawach teleinformatyki;
- 9) odtwarzać dane z kopii bezpieczeństwa modułu PS2O_KW, i PS2O_KZ;

- 10) nie ujawniać nikomu, poza właściwym konsulem oraz dyrektorem komórki organizacyjnej właściwej w sprawach konsularnych, oraz osobom przez niego upoważnionym, informacji dotyczących wykorzystania PS2O przez użytkowników oraz przesyłanych przez nich treści;
- 11) wykonywać inne czynności wskazane w „Instrukcji zarządzania systemami informatycznymi”.

Obowiązki Administratorów systemów wspierających

§ 8

1. Administratorzy systemów wspierających są obowiązani:
 - 1) ściśle współpracować z Administratorem systemu;
 - 2) powiadomić Administratora systemu o wystąpieniu zdarzeń grożących utratą ciągłości działania lub bezpieczeństwu PS2O;
 - 3) we współpracy z Administratorem systemu podejmować niezwłocznie czynności w celu usunięcia awarii;
 - 4) wykonywać inne czynności wskazane w „Instrukcji zarządzania systemami informatycznymi”.
2. Administratorzy systemów wspierających są obowiązani do przestrzegania zasad użytkowania PS2O określonych w instrukcji, wytycznych i poleceniach, o których mowa w § 3 ust. 2.

Obowiązki Regionalnych Administratorów Systemów Teleinformatycznych w placówkach zagranicznych

§ 9

Regionalny Administrator Systemów Teleinformatycznych jest obowiązany:

- 1) przestrzegać zasad użytkowania, określonych w instrukcji, o której mowa w § 3 ust. 2 oraz stosować wytyczne i polecenia wydane w tym zakresie przez dyrektora komórki organizacyjnej właściwej w sprawach teleinformatyki oraz działającego z jego upoważnienia Administratora systemu;
- 2) administrować modulem PS2O_KZ w placówkach objętych zakresem odpowiedzialności administratora;
- 3) przygotować infrastrukturę informatyczną placówki objętej zakresem odpowiedzialności administratora do przeprowadzenia wdrożenia PS2O;
- 4) powiadomić Administratora systemu o wystąpieniu zdarzeń zagrażających utracie ciągłości działania, bezpieczeństwu lub danych w module PS2O_KZ;
- 5) w uzgodnieniu z Administratorem systemu, zainstalować i skonfigurować sprzęt oraz oprogramowanie niezbędne do pracy modułu PS2O_KZ;

- 6) w uzgodnieniu z Administratorem systemu, aktualizować oprogramowanie systemów i aplikacji wspierających, które nie są zdalnie zarządzane;
- 7) podejmować czynności w celu wyjaśnienia wszelkich zaobserwowanych nieprawidłowości w działaniu modułu PS2O_KZ;
- 8) wykonywać i odtwarzać kopie bezpieczeństwa modułu PS2O_KZ i zawarty w nim danych;
- 9) powiadomić Administratora Bezpieczeństwa Informatyki oraz Administratora Bezpieczeństwa Systemu Informatycznego o przypadkach wystąpienia ryzyka naruszenia zasad ochrony danych osobowych przetwarzanych w systemie PS2O zgodnie z „Instrukcją postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych”.

Obowiązki użytkownika

§ 10

1. Użytkownik jest obowiązany do:

- 1) przestrzegania zasad użytkowania, określonych w instrukcji, o której mowa w § 3 ust. 2 oraz stosowania wytycznych i poleceń wydanych w tym zakresie przez dyrektora komórki organizacyjnej właściwej w sprawach teleinformatyki oraz działającego z jego upoważnienia Administratora systemu;
- 2) zapoznania się z dokumentacją użytkownika PS2O w części odpowiadającej zakresowi obowiązków;
- 3) uczestnictwa w szkoleniach organizowanych w placówkach zagranicznych oraz w Ministerstwie Spraw Zagranicznych;
- 4) korzystania z PS2O wyłącznie w celu realizacji zadań służbowych;
- 5) zgłaszania do Centrum Wsparcia Technicznego niestandardowego zachowania PS2O lub stwierdzenia błędów rejestracji danych, które nie wynikają z błędów obsługi;
- 6) korzystania z PS2O w taki sposób, aby ograniczyć ryzyko nieuprawnionego zapoznania się osób postronnych z informacjami przetwarzanymi za jego pomocą;
- 7) ochrony karty dostępowej i numeru PIN oraz PUK do PS2O;
- 8) okresowej, nie rzadziej, niż co 40 dni, zmiany numeru PIN oraz PUK do karty dostępowej;
- 9) wylogowywania się oraz zabezpieczenia karty dostępowej PS2O za każdym razem, gdy opuszcza stanowisko pracy;
- 10) powiadomić Administratora Bezpieczeństwa Informatyki oraz Administratora Bezpieczeństwa Systemu Informatycznego o przypadkach wystąpienia ryzyka naruszenia zasad ochrony danych osobowych przetwarzanych w systemie PS2O zgodnie z „Instrukcją postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych”.

2. Użytkownik powinien przestrzegać następujących ograniczeń:
 - 1) zabronione jest samowolne instalowanie i/lub usuwanie oprogramowania komputerowego;
 - 2) zabroniona jest samowolna zmiana ustawień i modyfikacji systemu operacyjnego komputera i/lub parametrów PS2O;
 - 3) zabronione jest samowolne przełączanie kabli sieciowych, dokonywanie innych modyfikacji konfiguracji sprzętowej stanowiska pracy.
3. Użytkownik odpowiada za wszelkie działania, które zostaną zarejestrowane w PS2O przy pomocy jego danych dostępowych.

Zasady udzielania dostępu do PS2O

§ 11

1. Dostęp do PS2O jest udzielany indywidualnemu pracownikowi, którego zakres realizowanych zadań służbowych uzasadnia konieczność udzielenia takiego dostępu.
2. W przypadku ustania okoliczności wymienionej w ust. 1, dostęp do PS2O powinien zostać cofnięty.
3. Zakres udzielonego dostępu do obsługi PS2O powinien być ściśle dopasowany do zakresu obowiązków służbowych realizowanych przez pracownika określonych przez kierownika placówki, dyrektora komórki organizacyjnej właściwej do spraw konsularnych lub dyrektora komórki właściwej do spraw osobowych.
4. O wszelkich zmianach dotyczących udzielania dostępu do PS2O i/lub zmianach zakresu uprawnień nadanych pracownikowi, a także cofnięcia tych uprawnień decyduje kierownik placówki, dyrektor komórki organizacyjnej właściwej do spraw konsularnych lub dyrektor komórki właściwej do spraw osobowych.
5. Użytkownik systemu PS2O powinien posiadać stosowne upoważnienie do przetwarzania danych osobowych wydane zgodnie zasadami określonymi w „Polityce Bezpieczeństwa Danych Osobowych” oraz „Instrukcji nadawania upoważnień do przetwarzania danych osobowych w Ministerstwie Spraw Zagranicznych i placówkach zagranicznych”.

6. Udzielenie dostępu oraz definiowanie zakresu uprawnień do PS2O dla pracownika określa kierownik placówki, dyrektor komórki organizacyjnej właściwej do spraw konsularnych lub dyrektor komórki organizacyjnej właściwej do spraw osobowych, a realizuje Administrator systemu lub Regionalny Administrator Systemów Teleinformatycznych.

Bezpieczeństwo PS2O

§ 12

1. Administrator systemu odpowiada za bezpieczeństwo PS2O, w tym, w uzgodnieniu z Administratorem wspierającym w zakresie bezpieczeństwa teleinformatycznego, proponuje reguły bezpieczeństwa i po ich zatwierdzeniu przez dyrektora komórki organizacyjnej właściwej w sprawach teleinformatyki wdraża je w PS2O.
2. Wszystkie osoby, o których mowa w niniejszym zarządzeniu zobowiązane są do przestrzegania zasad określonych w przepisach powszechnie obowiązujących oraz aktach wewnętrznych dotyczących ochrony danych osobowych, a przede wszystkim: „Polityce Bezpieczeństwa Danych Osobowych”, „Instrukcji nadawania upoważnień do przetwarzania danych osobowych”, „Instrukcji zarządzania systemami informatycznymi” oraz „Procedurami uwierzytelniania w Paszportowym Systemie Obsługi Obywatela (PS2O)”.

Przepisy końcowe

§ 13

Dyrektor komórki organizacyjnej właściwej w sprawach teleinformatyki jest obowiązany do opracowania i wdrożenia, w terminie 30 dni od dnia wejścia w życie zarządzenia, instrukcji, o której mowa w § 3 ust. 2.

§ 14

Zarządzenie wchodzi w życie z dniem podpisania.

Dyrektor Generalny Służby Zagranicznej

Jarosław Czubiński