Wymogi i zalecenia dla Użytkowników uzyskujących dostęp do Rejestru zastrzeżeń numerów PESEL w drodze weryfikacji (Projekt)

Metryka dokumentu

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Właściciel | Minister właściwy do spraw informatyzacji | | | |
| Tytuł dokumentu | Wymogi dla Użytkowników uzyskujących dostęp do Rejestru zastrzeżeń numerów PESEL w drodze weryfikacji | | | |
| Tryb zatwierdzenia: | Dokument zatwierdza Dyrektor Centralnego Ośrodka Informatyki | | | |
| Stan |  | | Daty obowiązywania |  |
| Założenia | Dokument określa podstawowe wymogi i zalecenia dla Użytkowników systemu uzyskujących dostęp do Rejestru zastrzeżonych numerów PESEL w drodze weryfikacji, w tym stacji roboczych wykorzystywanych przez Użytkowników. | | | |
| Powiązania |  | | | |
| Adresaci | Użytkownicy systemu Rejestru zastrzeżeń numerów PESEL | | | |
| Klasyfikacja informacji |  | | Dystrybucja |  |
| Historia dokumentu | Wersja | Data | Autor | Opis zmian |
| 0.1 | 06.06.2023 | Zespół ZZC COI | Projekt |
| 0.2 | 06.11.2023 | Zespół ZZC COI | Zmiany w projekcie dokumentu |
|  |  |  |  |

Spis treści

[1. Postanowienia ogólne 4](#_Toc150177111)

[2. Dokumentacja bezpieczeństwa informacji 5](#_Toc150177112)

[3. Wymagania dotyczące podłączenia infrastruktury Podmiotu uprawnionego 5](#_Toc150177113)

[4. Rozliczalność działań na urządzeniach i w systemach teleinformatycznych Podmiotów uprawnionych 6](#_Toc150177114)

[5. Wymagania dotyczące ochrony fizycznej 6](#_Toc150177115)

[5.1. Wymagania wynikające z przepisów prawa 6](#_Toc150177116)

[5.2. Zalecenia Właściciela systemu 6](#_Toc150177117)

[6. Podstawowe wytyczne dla stacji roboczych i nośników informacji 6](#_Toc150177118)

[7. Zalecenia w przypadku użytkowania komputerów przenośnych   
jako stacje robocze 10](#_Toc150177119)

[8. Podstawowe zasady bezpieczeństwa 11](#_Toc150177120)

[9. Nadzór i kontrola nad Podmiotami uprawnionymi 11](#_Toc150177121)

[10. Postanowienia końcowe 11](#_Toc150177122)

## Postanowienia ogólne

1. Adresatami dokumentu są Użytkownicy systemu, o których mowa art. 23m ust. 1 ustawy o ewidencji ludności (zwani dalej: „Podmiotami uprawnionymi”), którym udostępniane są dane z rejestru zastrzeżonych numerów PESEL (zwanego dalej: „Rejestrem”), za pomocą urządzeń teletransmisji danych, w drodze weryfikacji, a mianowicie:
2. organy administracji publicznej, sądy i prokuratura;
3. Policja, Straż Graniczna, Straż Marszałkowska, Służba Więzienna, Służba Kontrwywiadu Wojskowego, Służba Wywiadu Wojskowego, Krajowa Administracja Skarbowa, Żandarmeria Wojskowa, Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, Służba Ochrony Państwa, Centralne Biuro Antykorupcyjne, Szef Krajowego Centrum Informacji Kryminalnych, Inspektor Nadzoru Wewnętrznego, organy wyborcze i straże gminne (miejskie);
4. komornicy sądowi - wyłącznie w zakresie niezbędnym do prowadzenia przez nich postępowania egzekucyjnego lub zabezpieczającego albo wykonywania postanowienia o zabezpieczeniu spadku lub sporządzania spisu inwentarza;
5. państwowe i samorządowe jednostki organizacyjne oraz inne podmioty - w zakresie niezbędnym do realizacji zadań publicznych określonych w odrębnych przepisach;
6. Polski Czerwony Krzyż - w zakresie danych osób poszukiwanych;
7. osoby i jednostki organizacyjne, jeżeli wykażą w tym interes faktyczny;
8. podmioty, o którym mowa w art. 4 ust. 1 pkt 1, 17, 18 i 20 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe oraz instytucji utworzonej na podstawie art. 105 ust. 4 tej ustawy, np.: bank krajowy, instytucja kredytowa;
9. notariusz (*ustawie z dnia 14 lutego 1991 r. – Prawo o notariacie*);
10. dostawcy publicznie dostępnych usług telekomunikacyjnych (*ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne*);
11. spółdzielcze kasy oszczędnościowo-kredytowe (*ustawa z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych*);
12. kredytodawcy w rozumieniu art. 5 pkt 2 ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim;
13. dostawcy, o których mowa w art. 4 ust. 2 pkt 4, 6, 9 i 11 ustawy z dnia 19 sierpnia 2011r. o usługach płatniczych;
14. biura informacji gospodarczej, o których mowa w art. 5 ustawy z dnia 9 kwietnia 2010 r. o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych
15. Podmioty uprawnione przed wydaniem przez ministra właściwego do spraw informatyzacji zgody w drodze decyzji administracyjnej na udostępnianie danych za pomocą urządzeń teletransmisji danych w drodze weryfikacji muszą spełnić następujące wymogi:
16. posiadać urządzenia lub systemy teleinformatyczne przeznaczone do komunikowania się pomiędzy uprawnionymi podmiotami a rejestrem zastrzeżonych PESEL-i, umożliwiające identyfikację osoby uzyskującej dane z rejestru, zakres oraz datę ich uzyskania;
17. posiadać zabezpieczenia techniczne i organizacyjne właściwe dla przetwarzania danych osobowych, w szczególności uniemożliwiające dostęp osób nieuprawnionych do przetwarzania danych osobowych i wykorzystanie danych niezgodnie z celem ich uzyskania.
18. W celu zapewnienia spełnienia wskazanych powyżej warunków zostały poniżej określone zalecenia dotyczące bezpieczeństwa informacji.
19. Bezpieczeństwo informacji rozumiane jest jako zachowanie takich właściwości informacji i systemu informacyjnego, jak:
20. poufność – właściwość polegająca na tym, że informacja nie jest udostępniana ani ujawniana nieautoryzowanym podmiotom (osobom, podmiotom lub procesom);
21. integralność – właściwość polegająca na zapewnieniu dokładności i kompletności;
22. dostępność – właściwość bycia dostępnym i użytecznym na żądanie autoryzowanego podmiotu;
23. rozliczalność – właściwość systemu pozwalająca przypisać określone działanie w systemie do podmiotu oraz umiejscowić je w czasie;
24. niezaprzeczalność – zdolność do udowodnienia, że wystąpiły deklarowane zdarzenia lub działania oraz, że wywołał je dany podmiot;
25. autentyczność – właściwość polegająca na tym, że podmiot jest tym, za kogo się podaje;
26. niezawodność – właściwość oznaczająca spójne, zamierzone zachowanie i skutki.

## Dokumentacja bezpieczeństwa informacji

Podmioty uprawnione są zobowiązane opracować i wdrożyć dokumentację bezpieczeństwa informacji, w tym dokumentację gwarantującą wdrożenie odpowiednich środków organizacyjnych i technicznych gwarantujących bezpieczeństwo przetwarzania danych osobowych, stosownie do art. 32 RODO.

## Wymagania dotyczące podłączenia infrastruktury Podmiotu uprawnionego

1. Informacja o zastrzeżeniu numerów PESEL będzie gromadzona w oddzielnym rejestrze, dzięki czemu dostęp do niego nie będzie wymagał korzystania z dedykowanej sieci dostępowej (sieci wydzielonej).
2. Dostęp do rejestru zastrzeżonych numerów PESEL w drodze weryfikacji jest dostępny za pomocą usługi WebService udostępnionej „na zewnątrz”.
3. Dostęp do Rejestru wymaga podania publicznego adresu/adresów IP, z którego będzie następowało połączenie urządzenia lub systemu teleinformatycznego Podmiotu uprawnionego z Rejestrem oraz wydania klucza API dla Podmiotu uprawnionego.

## Rozliczalność działań na urządzeniach i w systemach teleinformatycznych Podmiotów uprawnionych

1. Należy wdrożyć takie mechanizmy, aby działania poszczególnych użytkowników wewnętrznych u Podmiotów uprawnionych mogły być jednoznacznie powiązane z tymi użytkownikami, tak aby mogli oni zostać pociągnięci do odpowiedzialności za swoje działania.
2. Należy okresowo przeglądać, chronić i przechowywać rejestry logów systemu informatycznego w zakresie niezbędnym do umożliwienia monitorowania, analizy, badania i zgłaszania bezprawnych, nieautoryzowanych lub nieodpowiednich działań.
3. Logi powinny być przechowywane w formacie pozwalającym na odczyt oraz eksport danych do powszechnych aplikacji biurowych lub innych programów użytkowych.
4. Logi powinny być przechowywane przez okres wskazany przepisami obowiązującego prawa.

## Wymagania dotyczące ochrony fizycznej

### Wymagania wynikające z przepisów prawa

Podmioty uprawnione zobowiązane są zapewnić poziom ochrony fizycznej pomieszczeń, w których są zlokalizowane stacje robocze uzyskujące dostęp do Rejestru w sposób zgodny z przepisami prawa, w tym dotyczącymi ochrony danych osobowych.

### Zalecenia Właściciela systemu

Ponadto w uregulowaniach wewnętrznych należy wziąć pod uwagę poniższe zalecenia:

1. Pomieszczenia powinny zapewniać bezpieczeństwo i takie rozmieszczenie sprzętu oraz dokumentów, aby uniemożliwić dostęp do informacji osobom nieupoważnionym i nie powinny być pomieszczeniami przechodnimi. Aby uniemożliwić dostęp do informacji osobom nieupoważnionym można stosować zabezpieczenia fizyczne stanowisk pracy.
2. Powinna być wdrożona kontrola dostępu do pomieszczeń. Dostęp do pomieszczeńmogą mieć tylko osoby uprawnione. Inne osoby mogą przebywać w pomieszczeniachjedynie w obecności osób uprawnionych, za ich wiedzą i zgodą. Obecność innych osób w pomieszczeniu powinna być dokumentowana.

## Podstawowe wytyczne dla stacji roboczych i nośników informacji

1. Przez stację roboczą należy rozumieć służbowy komputer stacjonarny lub komputer przenośny (laptop) przeznaczony do bezpośredniej pracy wykonywanej przez pracownika Podmiotu uprawnionego (komputer który nie jest serwerem, tzn. nie pracuje na potrzeby sieci, lecz korzysta z jej zasobów).
2. W poniższej tabeli zgromadzono listę zaleceń wraz z wyjaśnieniami i uwagami o zakresie ich stosowania.

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Zalecenie** | **Uwagi i wyjaśnienia do zaleceń** |
|  | Zalecany jest zainstalowany system operacyjny, np. Windows, Mac OS, Linux lub inny wspierany przez producenta oraz posiadający możliwość użycia oprogramowania antywirusowego oraz mechanizmów szyfrowania danych. | System operacyjny musi być wspierany przez producenta w zakresie poprawek i aktualizacji zabezpieczeń oraz wspierać sterowniki urządzeń peryferyjnych niezbędnych do pracy.  Data i godzina systemowa musi być synchronizowana z wzorcowym źródłem czasu.  Użytkownicy stacji roboczych nie powinni mieć możliwości samodzielnego instalowania oprogramowania. |
|  | Cykliczne aktualizowanie systemu operacyjnego i oprogramowania. | Aktualizacja systemu operacyjnego oraz oprogramowania zgodnie z zaleceniami producentów powinna odbywać się w zakresie i w czasie ustalonym przez Podmiot uprawniony. |
|  | Oprogramowanie antywirusowe zapewniające bezpieczeństwo danych na stacji roboczej jak również bezpieczeństwo dostępu do usług z sieci zewnętrznych (np. sieci Internet). | Oprogramowanie powinno posiadać aktualne definicje i bazy antywirusowe.  Użytkownicy stacji roboczych nie mogą posiadać uprawnień do wykonania jakichkolwiek zmian konfiguracji zastosowanego oprogramowania antywirusowego lub jego wyłączenia. |
|  | Zapewnić konfigurację systemu operacyjnego stacji roboczej, aby na wszystkich poziomach obniżyć ryzyko ataku z zewnątrz do minimum. | Zalecane jest wdrożenie polityki bezpieczeństwa dla systemu operacyjnego stacji roboczych, uwzgledniającej m.in. wyłączenie zbędnych usług, zablokowanie nieużywanych portów, wyłączenie zbędnych protokołów, zmiana domyślnych poświadczeń.  Zaleca się zapewnienie integrację z kontrolerem domeny „Active-Directory” – dotyczy systemu Windows w celu np. auto konfiguracji (GPO), synchronizacji czasu.  Opcjonalnie: zapewniać integrację z systemem usług katalogowych w zakresie co najmniej odpowiadającym funkcjonalności integracji z kontrolerem domeny typu „Active-Directory” (dotyczy wszystkich systemów operacyjnych), |
|  | Uruchomienie stacji roboczej wymaga uwierzytelnienia w systemie operacyjnym. Każdemu użytkownikowi komputera należy założyć oddzielne konto. Wbudowane konto administratora należy używać tylko w przypadku wykonywania czynności administratora przez uprawnione osoby. Konta użytkownika nie mogą mieć uprawnień administratora lokalnego na stacji roboczej (dopuszczalne jest odstępstwo od tej zasady w uzasadnionych przypadkach, rozpatrywane indywidualnie przez przełożonego użytkownika stacji roboczej). | Zalecane jest wdrożenie centralnej polityki zarządzania mechanizmami uwierzytelniania oraz centralne zarządzanie stacjami roboczymi.  W przypadku uwierzytelnienia loginem i hasłem: długość hasła dla konta użytkownika powinna posiadać co najmniej 12 znaków (hasło złożone co najmniej z dużej litery, małej litery, cyfry i znaku specjalnego). Powinien być ustawiony także okres ważności hasła; długość hasła konta administratora lub użytkownika z uprawnieniami administratora musi posiadać co najmniej 14 znaków (hasło złożone co najmniej z: dużej litery, małej litery, cyfry i znaku specjalnego), powinien być ustalony okres ważności hasła. |
|  | Dane przechowywane na dysku stacji roboczej powinny być umieszczone w obszarze podlegającym szyfrowaniu lub być szyfrowane. | Zaleca się wdrożenie mechanizmów szyfrowania danych zawartych na dyskach stacji roboczych. |
|  | Niedozwolone jest przekazywanie poufnych informacji uwierzytelniających osobom trzecim. | Zalecane jest wprowadzenie systemu szkoleń dla osób użytkujących stacje robocze oraz wprowadzenie sankcji za niedopełnienie obowiązków w tym zakresie. |
|  | Na stacji roboczej powinien być ustawiony mechanizm automatycznej blokady po określonym czasie braku aktywności użytkownika. | W momencie odejścia od stacji roboczej użytkownik powinien być zobowiązany do każdorazowego blokowania dostępu do stacji roboczej za pomocą wylogowania konta użytkownika lub załączenia wygaszacza ekranu z hasłem (np. w przypadku komputera z systemem Windows naciśnięcie klawiszy: „Ctrl” + „Alt” + „Del” i wybranie przycisku „Zablokuj komputer” lub załączenie wygaszacza ekranu skrótem klawiszowym „Win” + „L”; w przypadku komputera z systemem Mac OS wejście w ikonę Apple w lewym górnym rogu, a następnie wybranie opcji "Blokuj Ekran" lub naciśnięcie klawiszy: Control + Command + Q). |
|  | Nośniki informacji zawierające dane osobowe powinny być przechowywane w sposób bezpieczny. Do likwidacji wydruków dokumentów i nośników cyfrowych powinny być stosowane odpowiednie niszczarki, stosownie do stopnia poufności informacji i rodzaju nośnika. Podmiot uprawniony powinien posiadać stosowne uregulowania wewnętrzne w tym zakresie. W przypadku niszczenia dokumentów lub nośników przez firmą zewnętrzną powinna być zawarta stosowna umowna. | Informacje przechowywane na nośnikach informacji powinny być przechowywane w miejscach zabezpieczonych przed dostępem osób nieupoważnionych.  Do likwidacji wydruków dokumentów i nośników informacji powinno się stosować niszczarki odpowiedniej klasy, zgodnie z wytycznymi aktualnych norm w zakresie niszczenia nośników, a także wytycznymi wynikającymi z przepisów prawa. |
|  | Zalecane jest, aby wszelkie działania serwisowe stacji roboczych przeprowadzane były pod nadzorem w sposób uniemożliwiający dostęp do informacji dla osób nieuprawnionych. | Wszelkie działania serwisowe realizowane przez osobę lub podmiot trzeci powinny być przeprowadzane pod nadzorem w siedzibie lub poza siedzibą po uprzednim przygotowaniu stacji roboczej w sposób uniemożliwiający dostęp do przetwarzanych z jej wykorzystaniem informacji. |

## Zalecenia w przypadku użytkowania komputerów przenośnych jako stacje robocze

1. Komputer przenośny powinien być przypisany do konkretnego użytkownika, który oświadcza, że ma świadomość zagrożeń, np. jego kradzieży, utraty lub możliwości ujawnienia danych.
2. Komputer przenośny powinien być odpowiednio zabezpieczany przed jego kradzieżą, przejęciem poufnych danych uwierzytelniających, zgodnie z powszechnie obowiązującymi zasadami bezpieczeństwa, uwzględniając co najmniej:
3. komputer nie może być pozostawiony bez opieki;
4. komputer musi być odpowiednio zabezpieczony w czasie transportu (np. przewożony tylko w bagażu podręcznym). Nie należy ich także pozostawiać bez nadzoru w takich miejscach jak przechowalnie bagażu, wnętrza samochodów lub innych miejscach o podwyższonym ryzyku utraty sprzętu.
5. Komputer przenośny może być wykorzystywany tylko zgodnie z przeznaczeniem i zakresem obowiązków przypisanych jego użytkownikowi i nie może być użyczany osobom trzecim/innym podmiotom.
6. Komputer przenośny nie powinien być wynoszony poza siedzibę Podmiotu uprawnionego bez uzyskania stosownej zgody.
7. Wszystkie zdarzenia i incydenty związane bezpieczeństwem, w szczególności: utrata sprzętu, utrata lub podejrzenie ujawnienia poufnych danych uwierzytelniających, powinny być niezwłocznie zgłaszane zgodnie z procedurą obsługi incydentów bezpieczeństwa informacji obowiązującą u Podmiotów uprawnionych.
8. W przypadku wykonywania pracy zdalnej, o której mowa w Kodeksie pracy, polegającej na realizowaniu czynności służbowych lub powierzonych zadań poza siedzibą Podmiotu uprawnionego za pomocą środków komunikacji elektronicznej, kwestia ta powinna być uregulowana w wewnętrznych aktach prawnych, w tym w obszarze bezpieczeństwa informacji. Zaleca się, aby:
9. dostęp do sieci wewnętrznej Podmiotu uprawnionego był realizowany poprzez usługę bezpiecznego połączenia za pośrednictwem sieci Internet, polegającą na wykorzystaniu szyfrowanego tunelu służącego do transmisji danych oraz silnym uwierzytelnianiu przy zachowaniu pełnej rozliczalności działań użytkowników (klient VPN);
10. na komputerze przenośnym był zainstalowany dedykowany system klienta VPN;
11. połączenie zdalne z siecią wewnętrzną Podmiotu uprawnionego realizowane za pomocą skonfigurowanego klienta VPN odbywało się z wykorzystaniem indywidualnego konta oraz hasła użytkownika, które w sposób jednoznaczny muszą zapewniać rozliczalność jego działań w systemach wewnętrznych Podmiotu uprawnionego.

## Podstawowe zasady bezpieczeństwa

1. Zaleca się stosowanie zasady „czystego biurka” – na „biurku” powinny znajdować się wyłącznie te dokumenty, które są niezbędne do wykonywania obowiązków służbowych.
2. Po zakończeniu pracy wszystkie dokumenty i nośniki, które były wykorzystywane do realizacji zadań, powinny być zabezpieczone przed dostępem osób trzecich.
3. Ekran monitora powinien być ustawiony w taki sposób, by osoby trzecie nie miały możliwości wglądu do wyświetlanych treści na ekranie.
4. Wszystkie dokumenty, które są drukowane, skanowane, bądź kopiowane powinny być niezwłoczne zabrane z urządzenia drukującego/skanującego. Zalecane jest takie ustawienie drukarki aby nie było możliwości podejrzenia bądź pobrania wydruków przez osoby nieuprawnione.
5. Po zakończeniu pracy należy zamknąć wszystkie aktywne sesje oraz wylogować się z systemu lub aktywować oprogramowanie blokujące klawiaturę i wygaszacz ekranu zabezpieczony hasłem.

## Nadzór i kontrola nad Podmiotami uprawnionymi

1. Minister właściwy do spraw informatyzacji, na podstawie art. 57 ustawy o ewidencji ludności, może przeprowadzać kontrolę Podmiotów uprawnionych, którym udostępniane są dane z Rejestru, za pomocą urządzeń teletransmisji danych, w drodze weryfikacji, w zakresie spełniania przez te podmioty warunków, o których mowa w art. 48 ust. 1 pkt 1 i 2 ww. ustawy.
2. Minister właściwy do spraw informatyzacji odmawia wyrażenia zgody na udostępnienie danych za pomocą urządzeń teletransmisji danych w drodze weryfikacji albo cofa zgodę na ich udostępnienie, jeżeli nie zostały spełnione warunki określone w art. 23m ustawy o ewidencji ludności.

## Postanowienia końcowe

1. Za dalsze przetwarzanie danych uzyskanych za pomocą urządzeń teletransmisji danych w drodze weryfikacji odpowiedzialność ponosi Podmiot uprawniony, który je uzyskał.
2. W przypadku naruszenia ochrony danych osobowych w związku z uzyskiwanym dostępem do Rejestru, odpowiedzialność za te naruszenia ponosi Podmiot uprawniony.