



Polish VACC Polityka prywatności Ochrona danych osobowych

polski

SPIS TREŚCI

Wykaz zmian	3
1. Podsumowanie	4
1.1. Definicje	4
2. Wstęp	4
2.1. Cel ustanowienia polityki prywatności	4
2.2. Rodzaj danych	5
2.3. Rodzaj danych zbieranych przez Polish VACC bezpośrednio	5
2.4. Rodzaj danych zbieranych przez strony trzecie	5
2.5. Postanowienia polityki	5
3. Odpowiedzialność	6
3.1. Zarząd VACC	6
3.2. Wewnętrzny Inspektor Ochrony Danych Osobowych	6
3.3. Dyrektorzy poszczególnych departamentów	6
3.4. Asystenci zarządu i inni oddelegowani	6
4. Bezpieczeństwo	6
4.1. Zakres polityki bezpieczeństwa	6
4.2. Podejmowane kroki	6
4.3. Zagrożenia	7
5. Zapisywanie i przechowywanie danych	7
5.1. Zakres przechowywanych danych	7
5.2. Aktualizacja przechowywanych danych	7
5.3. Przechowywane dane	7
5.4. Okres przechowywania danych	7
5.5. Archiwizacja	8
6. Przejrzystość ochrony danych	8
7. Prawo dostępu do informacji	8
7.1. Odpowiedzialność PL-VACC	8
7.2. Procedura składania żądania	8
7.3. Weryfikowanie tożsamości	8
7.4. Opłaty	9
8. Prawo do usunięcia danych (bycia zapomnianym)	9
9. Podstawy prawne	9
10. Zmiany do tej polityki	9
10.1. Procedura zmiany	9

WYKAZ ZMIAN

Nr zmiany	Nr strony	Opis zmiany	Data
		Wydanie pierwsze	11.06.2020
1a	4	Usunięcie VATED; Wprowadzenie VATEMEA	20.11.2020
1b	7		
1c	9		
2	7	Błąd typograficzny (cztery)	

1. PODSUMOWANIE

1.1. Definicje

VATSIM – Virtual Air Traffic Simulation Network to organizacja non-profit zarządzająca dedykowaną, ogólnosiwiatową, wirtualną, lotniczą siecią, udostępniającą oprogramowanie potrzebne do latania na programowych symulatorach lotu w wirtualnej przestrzeni powietrznej¹. Informacje o organizacji dostępne są pod adresem <https://vatsim.net/>

VATEMEA – VATSIM Europe, Middle East and Africa Region – komórka organizacyjna VATSIM regionu europejskiego, afrykańskiego i Bliskiego Wschodu. Dodatkowe informacje znaleźć można pod adresem <https://vatsim.eu/>

VATEUD – VATSIM European Division – dywizja kontynentalnej części Europy VATEMEA. Dodatkowe informacje znaleźć można pod adresem <https://vateud.net/>

Polish VACC – Polish Virtual Area Control Centre – zwanym też PL-VACC, to ukonstytuowany członek dywizji VATEUD odpowiadający za wirtualną przestrzeń FIR Warszawa (EPWW) w sieci VATSIM. Dodatkowe informacje znaleźć można pod adresem <https://pl-vacc.org.pl/>

Zarząd PL-VACC – osoby nadzorujące w rozumieniu §2 oraz §3 Konstytucji Polish VACC z dnia 10 października 2019r.

Kanały komunikacyjne – sposoby komunikowania się członków Polish VACC z osobami odpowiedzialnymi za przetwarzanie Państwa danych osobowych w PL-VACC. Określone kanały komunikacyjne Polish VACC to:

- e-mail – komunikacja pocztą elektroniczną z wszystkimi adresami z domeny pl-vacc.org.pl,
- forum – forum dostępne pod adresem forum.pl-vacc.org.pl,
- Discord – oficjalny kanał PL-VACC na platformie Discord,
- platformy komunikacyjne – wszystkie formularze interaktywne dostępne na witrynach strony pl-vacc.org.pl.

Autoryzowany członek PL-VACC – osoba, której przyznano dostęp do danych objętych ochroną niniejszym dokumentem

Rozumienie słów kluczowych w tym dokumencie należy interpretować w następujący sposób:

- **MUSI** oznacza, że to zachowanie się (określona reguła, wymaganie) jest absolutnym wymogiem, alternatywnie: WYMAGA SIĘ, NALEŻY
- **NIE MOŻE** oznacza, że określone zachowanie się jest absolutnie zakazane, alternatywnie: NIE NALEŻY
- **POWINIEN** oznacza, że określone zachowanie się jest rekomendowane, a więc jedynie w ściśle określonych okolicznościach, jeżeli istnieją określone powody, określone zachowanie może być pominięte, alternatywnie: REKOMENDUJE SIĘ,
- **NIE POWINIEN** oznacza, że rekomenduje się nie wykonywać określonego zachowania, a więc zachowanie to jest dopuszczalne jedynie w określonych okolicznościach, alternatywnie: ODRADZA SIĘ, NIE REKOMENDUJE SIĘ,
- **MOŻE** oznacza, że określone zachowanie jest opcjonalne, a więc skutki tego realizacji lub pominięcia określonego zachowania są całkowicie neutralne, alternatywnie: OPCJONALNIE

Opracowano na podstawie specyfikacji wymagań RFC-2119.

2. WSTĘP

2.1. Cel ustanowienia polityki prywatności

Polityka prywatności i określenie ochrony danych osobowych mają na celu:

- zastosować się do prawa określonego w *Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie*

¹ Źródło: <https://pl.wikipedia.org/wiki/VATSIM>

o ochronie danych) oraz Ustawie z dnia 14 grudnia 2018r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125),

- zastosować się do obowiązku określonego przez VATSIM Data Protection and Data Handling Policy z dnia 25 maja 2018r, zmianami z dnia 9 czerwca 2020r oraz późniejszymi,
- zachowania dobrych praktyk ochrony danych osobowych członków oraz zarządu oraz wszystkich innych, którzy korzystają z usług Polish VACC

2.2. Rodzaj danych

Polish VACC gromadzi personalne dane osobowe swoich członków zarówno bezpośrednio, jak i za użyciem przekazywania danych stron trzecich.

2.3. Rodzaj danych zbieranych bezpośrednio

Podczas korzystania z naszych usług gromadzone są dodatkowe dane na Państwa temat. To pozwala nam zapewnić sprawne funkcjonowanie naszych usług i zapewnić pożądane wrażenia użytkownika. Dane te obejmują:

- zapisywanie i archiwizacja postów, wypowiedzi, zapisanych ustawień oraz wypełnionych formularzy, ankiet i głosowań zamieszczonych na kanałach komunikacyjnych Polish VACC,
- informacje o adresie IP wykorzystywanych w kanałach komunikacyjnych Polish VACC,
- zapisy postępów w treningach szkoleń prowadzonych przez Polish VACC,
- historię postępowań dyscyplinarnych,
- komunikację pomiędzy członkami, także tymi spoza zarządu.

Kanały komunikacyjne, w tym nasze forum, mają funkcję zbierania dowolnych danych w postaci dowolnego tekstu. Wszelkie dane osobowe dobrowolnie przesłane w ten sposób przez osoby fizyczne (np. dane osobowe, takie jak numery telefonów lub adresy) będą przechowywane, nawet jeśli zostaną ukryte przed dostępem publicznym. Dane te są wówczas dostępne tylko dla ograniczonej liczby upoważnionych osób.

2.4. Rodzaj danych zbieranych przez strony trzecie

Gdy członek korzysta z usług Polish VACC lub gdy prosi o dołączenie do oddziału Polish VACC dywizji VATEUD, dane są przekazywane z VATSIM lub innych stron trzecich poprzez kanały wewnętrznej komunikacji do Polish VACC w celu zapewnienia sprawnego funkcjonowania naszych usług oraz w celu zapewnienia najwyższych standardów dostarczanych usług. Dane te obejmują:

- pełne imię i nazwisko,
- numer identyfikacyjny w sieci VATSIM,
- adres e-mail,
- wirtualny stopień kontrolera ATC i/lub wirtualny stopień Pilota przydzielony w sieci VATSIM,
- zajmowane stanowiska w strukturach sieci VATSIM, wraz z przydzielonym zakresem obowiązków,
- dane dotyczące ram czasowych i długości trwania logowań wraz z użytymi znakami wywoławczymi podczas podłączenia do sieci VATSIM.

W przypadku korzystania z oficjalnego serwera komunikatora Discord, Polish VACC zbiera następujące dane:

- Unikalny numer identyfikacyjny ID oraz nazwa własna użytkownika przypisana do konta komunikatora Discord,

2.5. Postanowienia polityki

Polish VACC zobowiązuje się do:

- przestrzegania celów wymienionych w pkt 2.1 oraz dobrych praktyk wynikających z przetwarzania danych osobowych,
- przestrzegania praw jednostki, w tym:
 - prawa dostępu do informacji,
 - prawa do sprostowania,
 - prawa do sprzeciwu,
 - prawa do zapomnienia,
- prowadzenia transparentnej polityki prywatności,

- zapewnienia instrukcji postępowania osobom odpowiedzialnym za przetwarzanie danych w celu prowadzenia działań zgodnych z niniejszą polityką,
- informowania osób, których dane są przetwarzane, o wszelkich możliwościach lub podejrzeniach bezprawnego ujawnienia ich danych osobowych,

3. ODPOWIEDZIALNOŚĆ

3.1. Zarząd VACC

Ogólną odpowiedzialność za ochronę danych osobowych i zgodność odpowiednich standardów usług prowadzonych przez PL-VACC z niniejszą polityką prywatności ponosi Zarząd PL-VACC. Aktualny skład zarządu znajduje się pod adresem: <https://pl-vacc.org.pl/newvacc/aboutus.php>

3.2. Wewnętrzny Inspektor Ochrony Danych Osobowych

Osobą odpowiedzialną za czuwaniem nad przestrzeganiem niniejszej polityki prywatności zostaje wyznaczony Wewnętrzny Inspektor Ochrony Danych Osobowych (ang. Data Protection Officer). Obecny Wewnętrzny Inspektor Ochrony Danych Osobowych wskazany jest pod adresem:

<https://pl-vacc.org.pl/newvacc/aboutus.php>

3.3. Dyrektorzy poszczególnych departamentów

Poszczególni członkowie zarządu, odpowiedzialni za niżej wymienione oddziały działalności PL-VACC, mają szczególny obowiązek nadzorowania innych osób uzyskujących dostęp do danych osobowych gromadzonych przez VATSIM:

- Dyrektor Szkoły Kontrolerów ACCPL2 – archiwum danych szkoleń wirtualnych kontrolerów
- Dyrektor Usług Internetowych ACCPL5 – dostęp i kontrola do przechowywanych danych
- Dyrektor ds. Marketingu ACCPL10 – dane i archiwizacja danych uczestników konkursów, zamówień itp.

Innym członkom Zarządu mogą od czasu do czasu zostać przydzielone obowiązki związane z kontrolą i przechowywaniem danych.

3.4. Asystenci zarządu i inni oddelegowani

Zarząd powołuje asystentów zarządu zgodnie z §3 ust 7 Konstytucją Polish VACC, a także czasem oddelegowuje swoje prace innym członkom PL-VACC na zasadzie wolontariatu. Wszyscy, których to dotyczy, są zobowiązani do przeczytania, zrozumienia i zaakceptowania wszelkich zasad i procedur odnoszących się do przetwarzania danych osobowych, którymi mogą się posługiwać w trakcie swojej pracy w ramach PL-VACC, jak wyszczególniono w niniejszej polityce. Polish VACC oczekuje najwyższego standardu wiarygodności wśród wszystkich z nim współpracujących. Osoby nieuprawnione nie mogą uzyskać dostępu do danych, chyba że istnieje ważny powód takiego dostępu związany z siecią.

4. BEZPIECZEŃSTWO

4.1. Zakres polityki bezpieczeństwa

Niniejsza sekcja dotyczy wszystkich usług i serwerów Polish VACC, należących do Polish VACC lub przekazanych na jego rzecz, w tym: serwerów danych osobowych, danych statystycznych lub serwerów WWW.

4.2. Podejmowane kroki

Polish VACC podejmuje standardowe kroki zabezpieczenia danych, takich jak szyfrowanie TLS podczas uzyskiwania dostępu do danych używając przeglądarki internetowej. Dodatkowe ustawienia zabezpieczeń są używane w celu

umożliwienia dostępu do serwera tylko autoryzowanym użytkownikom. Hasła (z wyłączeniem hasła sieci VATSIM, które nigdy nie jest przekazywane do Polish VACC) są przechowywane jako szyfrowane ciągi, uniemożliwiając ich wyświetlanie w postaci zwykłego tekstu.

4.3. Zagrożenia

Zidentyfikowano cztery podstawowe źródła zagrożenia bezpieczeństwa danych przechowywanych przez PL-VACC. Są to:

- ataki phishingowe, czyli celowe wymuszenie nieautoryzowanego dostępu do danych zapisanych na serwerze,
- nieautoryzowany dostęp złośliwego oprogramowania zainfekowanych systemów używanych przez autoryzowanych członków PL-VACC,
- błędy w oprogramowaniu, umożliwiające nieautoryzowany (nawet przypadkowy) dostęp do danych zapisanych na serwerze,
- dostęp nieautoryzowanych członków PL-VACC.

Likwidacja dwóch pierwszych zagrożeń polega na:

- sprawdzeniu wszystkich osób przed przyznaniem dostępu ze znajomości niniejszej polityki prywatności,
- zachęcanie autoryzowanych członków do przestrzegania dobrych praktyk bezpieczeństwa w swoich systemach osobistych.

Trzecie ryzyko ograniczane jest poprzez odpowiednią fazę przeprowadzanych testów wprowadzanego oprogramowania.

Ostatnie ryzyko jest ograniczane przez rejestrowanie dostępu i cofanie zmian wprowadzanych przez tych, którzy niewłaściwie wykorzystują przyznany wcześniej dostęp.

5. ZAPISYWANIE I PRZECHOWYWANIE DANYCH

5.1. Zakres przechowywanych danych

Większość danych używanych przez PL-VACC jest przekazywana bezpośrednio przez kanały wewnętrznej komunikacji VATSIM. Dane wskazane w punktach 2.3 i 2.4 niniejszej polityki są przechowywane tylko w przypadku uzasadnionej potrzeby, określonej w pkt. 9.

5.2. Aktualizacja przechowywanych danych

Dane osobowe przechowywane przez PL-VACC synchronizowane są w ramach kanałów wewnętrznej wymiany danych osobowych SSO (Single Sign-On). Aktualizacja danych nie odbywa się więc bezpośrednio na serwerach PL-VACC, otrzymywane są one z serwerów trzecich. Zainteresowany członek PL-VACC powinien skierować żądania aktualizacji danych do odpowiednich organów VATSIM.

5.3. Przechowywane dane

Dane są przechowywane w standardowych systemach plików i bazach danych. Dostęp do tych systemów jest kontrolowany przez bezpieczny, bezpośredni dostęp do aplikacji sterujących lub za pośrednictwem bezpiecznego interfejsu internetowego. Dostęp jest następnie kontrolowany i chroniony przed nieautoryzowanym dostępem za pomocą standardowych środków, takich jak kontrola dostępu oparta na ograniczeniu uprawnień dostępu poszczególnych kont użytkowników.

5.4. Okres przechowywania danych

Polish VACC jest zobowiązany do przechowywania danych zgodnych z Polityką ochrony danych i ich przetwarzania sieci VATSIM. Żądania usunięcia mogą być przetwarzane przez Polish VACC zgodnie z pkt. 9, jednakże usunięcie niektórych przetwarzanych danych wymagać może interwencji VATEUD, VATEMEA lub bezpośrednio VATSIM, gdyż żądanie może pozostawać poza uprawnieniami osób odpowiedzialnych za Polish VACC.

5.5. Archiwizacja

Archiwizacja danych przez Polish VACC nie obejmuje danych przechowywanych na serwerach innych, niż serwerów należących do Polish VACC. Dane na tych serwerach są przechowywane w określonym okresie czasu, a następnie archiwizowane zgodnie z sekcją 2.3 lub całkowicie usuwane.

6. PRZEJRZYSTOŚĆ OCHRONY DANYCH

Polish VACC dokłada wszelkich starań, aby wszyscy członkowie wiedzieli, jakie dane i w jakim celu są gromadzone ich dane osobowe.

Jak określono w niniejszym dokumencie, dane są gromadzone w celu zapewnienia sprawnego funkcjonowania Polish VACC, aby członkowie mogli wspólnie cieszyć się funkcjonalnością sieci VATSIM.

7. PRAWO DOSTĘPU DO INFORMACJI

7.1. Odpowiedzialność PL-VACC

Wnioski o udostępnienie informacji przetwarzanych danych osobowych leżą w kompetencji i są obowiązkiem wyznaczonego Wewnętrznego Inspektora Ochrony Danych Osobowych.

Inspektor ten musi spełnić żądania zgodne z nadesłanym wnioskiem w ciągu jednego miesiąca od otrzymania takiego wniosku.

Wewnętrzny Inspektor Ochrony Danych Osobowych potwierdza otrzymanie wniosku, odpowiadając niezwłocznie po otrzymaniu wniosku interesantowi, lub osobie przekazującej wniosek w imieniu interesanta, o rozpoczętym procesie przetwarzania wniosku interesanta. Na podstawie informacji zwrotnej dla interesanta o rozpoczętym procesie, można ustalić termin, od którego rozpoczyna się miesięczny okres zobowiązania do rozpatrzenia wniosku.

Jeżeli, niewymienione w tym dokumencie, okoliczności przeszkodzą Wewnętrznemu Inspektorowi Ochrony Danych Osobowych do rozpatrzenia wniosku, okres spełnienia żądań może zostać jednorazowo wydłużony o miesiąc, pod warunkiem poinformowania interesanta o zaistniałej sytuacji, wskazania dokładnego okresu wydłużenia oraz podania powodów wydłużenia okresu spełnienia żądań.

Wniosek może zostać odrzucony przez Wewnętrznego Inspektora Ochrony Danych Osobowych w przypadku, gdy:

- żądanie wypływa od osoby, której dane nie dotyczą (np. wniosek o nieswoje dane),
- występuje brak możliwości zweryfikowania tożsamości osoby występującej z żądaniem,
- nie odnosi się do danych przechowywanych przez PL-VACC określonych niniejszym dokumentem,
- odnosi się do danych usuniętych zgodnie z pkt. 5.5 niniejszej polityki.

7.2. Procedura składania żądania

Żądania o udostępnienie informacji przetwarzanych danych osobowych w formie wniosku powinny być kierowane na adres e-mail: staff@pl-vacc.org.pl.

Jeżeli jakkolwiek członek lub osoba odpowiedzialna otrzyma cokolwiek, co uznane może być za żądanie o udostępnienie danych, powinien niezwłocznie poinformować o tym Wewnętrznego Inspektora Ochrony Danych Osobowych.

7.3. Weryfikowanie tożsamości

W przypadku wysłania żądania o udostępnienie danych osobowych, należy potwierdzić swoją tożsamość w celu rozpoczęcia przetwarzania wniosku.

Wewnętrzny Inspektor Ochrony Danych Osobowych, przed przystąpieniem do rozpoczęcia procesu przetwarzania wniosku, ma w obowiązku dokonać weryfikacji tożsamości osoby kierującej wnioskiem. Inspektor ten nie może jednak,

w ramach potwierdzania tożsamości dopuścić się do przechowywania kolejnych danych identyfikujących i będących danymi osobowymi (np. nie może zażądać kserokopii dokumentu tożsamości, jednak może zażądać jego okazanie, także w formie cyfrowej)

Wyjątkiem od formalnego potwierdzania jest fakt osobistej znajomości osoby występującej z żądaniem przez Inspektora.

Poprawność zweryfikowania tożsamości jest obowiązkiem Inspektora, jednakże sposób sformalizowania potwierdzenia tożsamości leży na interesancie.

7.4. Opłaty

Polish VACC nie pobiera żadnych opłat za przetwarzanie lub udostępnianie danych w oparciu o żądania udostępnienia informacji przetwarzanych danych osobowych.

8. PRAWO DO USUNIĘCIA DANYCH (BYCIA ZAPOMNIANYM)

Działając w oparciu o obowiązujące prawo wymienione w pkt. 2.1, Polish VACC zobowiązuje się do usunięcia danych na wnioski interesanta. Wniosek z żądaniem o usunięcie danych przetwarzany jest na takich samych zasadach, jak prawo do uzyskania informacji opisanym w punkcie 7. Procedurę składania żądania, weryfikowania tożsamości oraz określenie opłat związanych z procedurą określa rozdział 7 niniejszej polityki.

Wnioski z żądaniem o usunięcie danych należy kierować na staff@pl-vacc.org.pl

9. PODSTAWY PRAWNE

Polish VACC zapewnia, że ma uzasadniony interes w gromadzeniu i przechowywaniu danych osobowych opisanych powyżej. Powody tego roszczenia są następujące:

- Polish VACC jest dobrowolną społecznością, będącą członkiem aktywnym VATEUD, VATEMEA oraz VATSIM, promującą symulacje lotów i wirtualną kontrolę ruchu lotniczego, a wszyscy członkowie, którzy chcą dołączyć, mają oczywiste zainteresowanie takimi działaniami.
- Zebrane dane to minimum wymagane do umożliwienia płynnego i optymalnego funkcjonowania VACC, wyłącznie dla przyjemności jego członków.
- Dane są niezbędne, aby umożliwić personelowi VATSIM w Polsce właściwe zarządzanie VACC, zarówno w codziennych operacjach, jak i w okolicznościach, w których członek (członkowie) może działać w sposób sprzeczny z zasadami i przepisami regulującymi VACC.

10. ZMIANY DO TEJ POLITYKI

Odpowiedzialnym za zgodność tego dokumentu zgodnie z obowiązującym prawem spoczywa na Wewnętrznym Inspektorze Ochrony Danych Osobowych.

10.1. Procedura zmiany

W przypadku konieczności zmian w niniejszym dokumencie, wyznacza się następującą procedurę:

- ewentualne zmiany do niniejszej polityki wymagają przegłosowania zarządu PL-VACC z prawem do głosowania zgodnie z §3 pkt 6 Konstytucji Polish VACC,
- zmianę uznaje się za przegłosowaną w momencie, gdy uzyska ona względną większość oddanych głosów,
- wejście zmian w życie nie może nastąpić wcześniej, niż 5 dni po zakończeniu głosowania,
- wejście zmian można określić wcześniej, niż 5 dni, lecz nie krócej niż 24 godziny po zakończeniu głosowania, w przypadku rażących uchybień w niniejszym dokumencie, wymagających natychmiastowych zmian. Takie zmiany wymagają kwalifikowanej większości bezwzględnej oddanych głosów, by uznać je za przegłosowane.

Informacja o trybie procesowania musi być podana do publicznej wiadomości na etapie konsultacyjnym, najpóźniej w dniu ogłoszenia głosowania, lecz nie później niż rozpoczęcie głosowania.

Projekt zmian winien być przedłożony zarządowi, który poddaje go pod głosowanie, przez Wewnętrznego Inspektora Ochrony Danych Osobowych, a w przypadku braku jego wyznaczenia, przez obecnego Dyrektora ACCPL1.