

# G Data Security 2012

Podręcznik użytkownika

Wszystkie prawa zastrzeżone. Oprogramowanie oraz pisemny materiał informacyjny chronione są prawami autorskimi. Dozwolone jest wykonanie jednej kopii bezpieczeństwa oprogramowania, która nie może być udostępniania osobom trzecim.

G Data Software Spółka z ograniczoną odpowiedzialnością zastrzega sobie wszelkie prawa, a w szczególności do publikacji, powielania, edycji i korzystania z oprogramowania. Żadna część niniejszego podręcznika nie może być w żadnej formie powielana, ani przechowywana w bazach danych lub też jakichkolwiek innych systemach przechowywania danych bez pisemnej zgody wydawcy. Wyjątkiem są cytaty w artykułach recenzujących.

G Data Software Sp. z o.o. nie ponosi odpowiedzialności za szkody spowodowane użytkowaniem programu. Treść podręcznika może ulec zmianie. Aktualna pomoc znajduje się na stronie internetowej [www.gdata.pl](http://www.gdata.pl).

ISBN 978-83-61624-14-1

G Data Software Sp. z o.o.  
ul. 28 Lutego 2, 78-400 Szczecinek  
tel. 094 3729 650  
faks 094 3729 659  
e-mail: [biuro@gdata.pl](mailto:biuro@gdata.pl)  
Bank Zachodni WBK S.A.  
63 1090 1711 0000 0001 0987 7149

Wydanie pierwsze, Szczecinek 2011  
Printed in Poland

G Data Software Sp. z o.o.

## Spis treści

<b>Rozdział I Wstęp</b>	<b>1</b>
<b>Rozdział II Pomoc techniczna</b>	<b>1</b>
<b>Rozdział III Instalacja programu</b>	<b>2</b>
<b>Rozdział IV Po instalacji</b>	<b>7</b>
<b>Rozdział V Centrum zabezpieczeń</b>	<b>8</b>
1 Licencja .....	12
2 Obciążenie CPU .....	13
<b>Rozdział VI Ochrona antywirusowa</b>	<b>14</b>
<b>Rozdział VII Sygnatury wirusów</b>	<b>19</b>
<b>Rozdział VIII Filtrowanie HTTP</b>	<b>21</b>
<b>Rozdział IX Ustawienia</b>	<b>23</b>
1 AntiVirus - Ustawienia .....	23
<b>Rozdział X Warto wiedzieć</b>	<b>33</b>

## **II** G Data Security

1 Instalacja pełna czy niestandardowa? .....	33
2 Płyta startowa .....	34
3 Ikonka paska zadań .....	36
4 Co to są aktualizacje sygnatur wirusów? .....	38
5 Co to jest aktualizacja oprogramowania? .....	39
6 Jak uaktualnić sygnatury wirusów? .....	39
7 Skanowanie .....	41
8 Wykrycie wirusa .....	43
9 Inicjatywa G Data Malware Information .....	44
10 Komunikat "not-a-virus" .....	46
11 Kwarantanna .....	48
12 Raporty .....	49
13 Licencje wielostanowiskowe .....	51
14 Kontynuacja licencji .....	52
15 Przeniesienie licencji na inny komputer .....	52
16 Deinstalacja programu .....	53

## **Rozdział XI Warunki licencji**

**54**

---

# 1 Wstęp

Drogi użytkowniku!

Dziękujemy za zakupienie oprogramowania G Data i mamy nadzieję, że produkt w pełni spełni Twoje oczekiwania. Poniższa dokumentacja ułatwi przeprowadzenie procesu instalacji i dostarczy Ci podstawowych informacji na temat działania produktu. Wszelkie zapytania, sugestie i zgłoszenia problemów prosimy kierować do Pomoc technicznej G Data.



Jeśli potrzebujesz informacji na temat konkretnej opcji, w każdej chwili możesz kliknąć przycisk Pomoc lub F1 aby otworzyć stronę pomocy odnoszącą się do bieżącego okna.

## 2 Pomoc techniczna

Masz problemy z zainstalowaniem programu? Program nie działa? Zgłoś problem do Pomocy technicznej G Data. Aby zgłosić problem do Pomocy technicznej, wyślij wiadomość z opisem problemu. Można również zgłosić problem telefonicznie.

Dobre przygotowanie do rozmowy przyspieszy proces udzielania pomocy i ułatwi kontakt z serwisantem.

## 2 G Data Security

---

- Przygotuj dane klienta (dane dostępu do aktualizacji, Numer rejestracyjny lub Numer klienta)
- Upewnij się, że oprogramowanie G Data Software jest zainstalowane na komputerze
- Zgromadź informacje na temat sprzętu i innego oprogramowania zainstalowanego w komputerze
- Przygotuj kartkę i coś do pisania

e-mail: [pomoc@gdata.pl](mailto:pomoc@gdata.pl)

telefon: 94 3729 650

Odpowiedzi na większość pytań znajdziesz w podręczniku użytkownika lub w pliku pomocy. Warto zajrzeć też na stronę internetową G Data Software i przejrzeć najczęściej zadawane pytania na stronie: [www.gdata.pl/pomoc](http://www.gdata.pl/pomoc).

## 3 Instalacja programu

Oprogramowanie G Data Software funkcjonuje prawidłowo na komputerach o następujących parametrach:

- System Windows 7 lub Vista (32/64-bit), od 1 GB RAM
  - System Windows XP z dodatkiem SP 2 (tylko 32-bit),
-

---

od 512 MB RAM

Jeśli jest to nowy komputer, lub masz pewność, że był wcześniej chroniony przez skuteczne oprogramowanie antywirusowe, odinstaluj bieżący program antywirusowy i przystąp do instalacji według poniższego opisu. Jeśli masz uzasadnione podejrzenie, że komputer mógł zostać zainfekowany, możesz przed instalacją wykonać skanowanie przy pomocy płyty startowej G Data. Szczegóły znajdziesz w rozdziale: Płyta startowa.

### Krok 1

Uruchom instalację jednym ze wskazanych sposobów, w zależności od nośnika, jakim dysponujesz:

- Płyta CD/DVD: Włóż płytę do napędu. Okno autostartu lub instalatora programu G Data otworzy się automatycznie.
- Pendrive USB: Włóż napęd USB do gniazda w komputerze. Okno autostartu lub instalatora programu G Data otworzy się automatycznie.
- Plik pobrany z Internetu: Kliknij dwukrotnie plik instalacyjny pobrany z Internetu aby uruchomić instalatora.

### Krok 2

Kliknij przycisk Instaluj. Kreator instalacji przeprowadzi Cię przez wszystkie etapy instalacji.

## 4 G Data Security

---

### Krok 3

Podczas instalacji program zapyta o metodę aktywacji produktu. Program będzie aktualizował się przez Internet po dokonaniu aktywacji.

- Chcę wprowadzić nowy numer rejestracyjny: Jeśli chcesz zarejestrować zakupiony numer rejestracyjny produktu G Data, wybierz tę opcję. Wypełnij formularz i kliknij przycisk Rejestracja online.

Po zarejestrowaniu dane dostępu do aktualizacji zostaną automatycznie wprowadzone do programu, a także wysłane na wskazany w formularzu adres e-mail.

W przypadku problemów z rejestracją, sprawdź, czy wpisujesz numer rejestracyjny poprawnie. Łatwo pomylić duże "I" (jak Irena) z cyfrą "1" lub małym "l" (jak lebioda). Podobnie: "B" i "8", "G" i 6, "O" i "0" czy "Z" i "2".

- Chcę wprowadzić dane dostępu: Jeśli Twój numer został wcześniej zarejestrowany, możesz od razu wprowadzić dane dostępu (użytkownik i hasło).

Dane dostępu znajdziesz w wiadomości e-mail potwierdzającej rejestrację.

Jeśli nie masz danych w zasięgu ręki, lub nie masz dostępu do wiadomości z potwierdzeniem rejestracji, kliknij przycisk Nie pamiętasz danych dostępu? Zostaniesz przeniesiony na stronę internetową

---

---

umożliwiająca ponowne wysłanie danych dostępu po wpisaniu adresu e-mail wskazanego w procesie rejestracji. W razie problemów z odzyskaniem danych skontaktuj się z Pomocą techniczną.

- **Wersja testowa:** Jeśli chcesz wypróbować oprogramowanie G Data, zarejestruj się bezpłatnie wypełniając formularz wersji trial nie wymagający wpisania numeru rejestracyjnego. Wpisz prawidłowy adres e-mail. Na ten adres zostaną wysłane dane do aktualizacji produktu.
- **Uaktywnię później:** Jeśli nie chcesz uaktywniać oprogramowania, lub chcesz to zrobić później, wybierz tę opcję. Produkt będzie w pełni funkcjonalny, ale nie będzie pobierał aktualizacji z Internetu. W celu uaktywnienia oprogramowania w późniejszym terminie, uruchom aktualizację. Program sam zaoferuje dostępne opcje aktywacji.

## 6 G Data Security

---

Oprogramowanie G Data skutecznie chroni Twój komputer dopiero po uaktywnieniu. Korzystanie z oprogramowania bez aktualizacji nie gwarantuje skutecznej ochrony.

### Krok 4

Po zakończeniu instalacji kreator poprosi o pozwolenie na ponowne uruchomienie komputera. Po restarcie systemu produkt jest gotowy do pracy.



Jeśli instalacja nie rozpoczyna się automatycznie: Może to oznaczać, że w Twoim systemie funkcja automatycznego uruchamiania jest wyłączona lub nie działa prawidłowo.

- Jeśli pojawi się okno wyboru autostartu systemu Windows, wybierz opcję Uruchom AUTOSTRT.EXE.
- Jeśli nie otwiera się żadne okno, otwórz Eksplorator Windows i z napędu z nośnikiem zawierającym wersję instalacyjną uruchom plik Setup lub Setup.exe.

Jeżeli chcesz odinstalować lub zainstalować poszczególne składniki programu, uruchom Panel sterowania systemu Windows i skorzystaj z polecenia Zmień dostępnego w aplecie Dodaj/Usuń programy (Windows XP) lub Programy i funkcje (Windows 7, Vista).

---

---

## 4 Po instalacji



Okno interfejsu oprogramowania G Data możesz otworzyć klikając ikonę programu na pulpicie. Widok Centrum zabezpieczeń informuje o stanie poszczególnych modułów zabezpieczających. Szczegóły znajdziesz w rozdziale Centrum zabezpieczeń.

Oprócz okna interfejsu programu G Data Software, masz do dyspozycji kilka innych możliwości skorzystania z zainstalowanego oprogramowania:

- **Szybkie skanowanie**  
Znalazłeś na dysku podejrzany plik? Chcesz szybko przeskanować plik pobrany z Internetu lub folder? Nie musisz uruchamiać okna programu G Data Software. Kliknij dany plik lub folder prawym klawiszem myszki i wybierz polecenie Skanuj programem G Data AntiVirus.



**Ikonka paska zadań:** Ikona programu umożliwia szybki dostęp do niektórych opcji programu. W razie potrzeby wyświetla znak ostrzeżenia informujący o potrzebie ingerencji użytkownika lub przypominający o wyłączonych czasowo zabezpieczeniach. Więcej szczegółów w rozdziale: Ikonka paska zadań.

## 8 G Data Security

---



**Niszczarka:** Narzędzie umożliwiające bezpowrotne usuwanie plików. Aby zniszczyć plik, przeciągnij go nad ikonę Niszczarki i upuść. Możesz również skorzystać z menu kontekstowego prawego klawisza. Narzędzie jest dostępne tylko w pakietach zabezpieczeń G Data. Nie znajdziesz go w produkcie G Data AntiVirus.

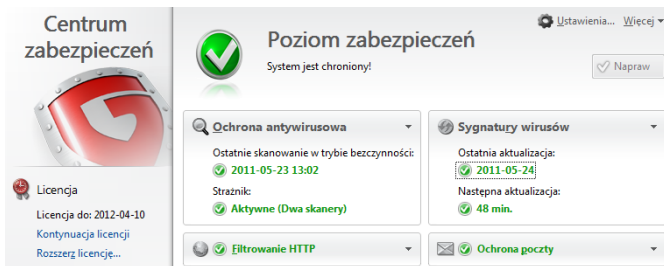


Po zainstalowaniu programu komputer uruchamia się inaczej niż zwykle: Możliwe, że płyta z programem G Data nadal znajduje się w napędzie, i zamiast systemu Windows uruchamia się system operacyjny z płyty startowej. Aby uruchomić system Windows, wyjmij płytę z napędu. Szczegóły na temat płyty startowej znajdziesz w rozdziale: Płyta startowa

## 5 Centrum zabezpieczeń

Po zainstalowaniu oprogramowania G Data Software ochrona komputera odbywa się całkowicie automatycznie. Uruchamianie Centrum zabezpieczeń jest niezbędne tylko w celu przeprowadzenia ręcznego skanowania danych lub modyfikacji ustawień.



---



The screenshot shows the Windows Security Center interface. On the left, there is a 'Centrum zabezpieczeń' logo and a license section. The main area is titled 'Poziom zabezpieczeń' and shows a green checkmark icon with the text 'System jest chroniony!'. Below this, there are four security components, each with a status indicator and a 'Napraw' button:

- Ochrona antywirusowa**: Ostatnie skanowanie w trybie bezczynności: 2011-05-23 13:02, Strażnik: Aktywne (Dwa skanery)
- Sygnatury wirusów**: Ostatnia aktualizacja: 2011-05-24, Następna aktualizacja: 48 min.
- Filtrowanie HTTP**
- Ochrona poczty**

Widok Centrum zabezpieczeń przedstawia stan poszczególnych składników ochrony w jednym oknie. Ikona poziomu zabezpieczeń informuje o stanie produktu.

-  Zielony kolor oznacza, że ustawienia zabezpieczeń są optymalne i system jest bezpieczny.
-  Czerwony kolor oznacza potencjalne zagrożenie dla systemu operacyjnego. Niezbędna jest natychmiastowa interwencja użytkownika.

Jeżeli wymagana jest ingerencja w ustawienia, przycisk Napraw jest podświetlony. Po kliknięciu przycisku Napraw, oprogramowanie automatycznie zmodyfikuje ustawienia lub podpowie co zrobić, tak aby komputer znów był bezpieczny.

Jeżeli ikona poziomu zabezpieczeń jest w kolorze

## 10 G Data Security

---

zielonym, przycisk Napraw wyłącza się i jest wyszarzony.

Po wykonaniu żądanych działań, możesz zamknąć Centrum zabezpieczeń. Przy opisach funkcji mogą się również pojawić następujące ikony:



Żółty kolor ikony poziomu zabezpieczeń informuje o potrzebie interwencji w ustawienia.



Jeśli dana funkcjonalność lub składnik programu jest wyłączony, przy jego opisie znajduje się taka właśnie ikona.

Modyfikacji ustawień i funkcji możesz dokonać przy pomocy przycisków dostępnych w sekcjach widocznych poniżej statusu zabezpieczeń.



Ustawienia: Ten przycisk otwiera okno ustawień dotyczących poszczególnych warstw ochrony. Szczegóły znajdziesz w rozdziale: Ustawienia.

Obok przycisku ustawienia znajdziesz menu Więcej umożliwiające wykonanie następujących czynności:



Pomoc: Otwiera plik pomocy programu G Data. Jeśli potrzebujesz informacji na temat konkretnej

---

opcji, w każdej chwili możesz kliknąć w danym oknie przycisk Pomoc lub klawisz F1 aby otworzyć stronę pomocy odnoszącą się do bieżącego okna.



**Raporty:** Widok raportów zawiera listę wszystkich raportów z działań programu. Klikając nagłówki poszczególnych kolumn, możesz posortować je według czasu rozpoczęcia, rodzaju, tytułu lub statusu.



**Nagraj płytę startową:** Możesz sporządzić płytę startową z aktualnymi bazami wirusów. Jest to możliwe również poprzez uruchomienie polecenia Tworzenie płyt startowych w grupie programowej menu Start. W odróżnieniu od oryginalnej płyty instalacyjnej z programem, płyta startowa skanuje przy użyciu aktualnych (w momencie jej utworzenia) sygnatur wirusów. Do utworzenia płyty startowej potrzebna jest czysta płyta. Kreator umożliwi także pobranie sygnatur wirusów przed nagraniem płyty. Opis działania płyty startowej znajdziesz w rozdziale: Jak działa płyta startowa?



**Uaktualnij pliki programu:** Jeśli dostępna jest aktualizacja plików programu G Data dla zainstalowanej wersji produktu, ten przycisk

umożliwia jej pobranie i zainstalowanie.

Więcej szczegółów na temat aktualizacji w rozdziale: Aktualizacje



Kliknij przycisk Informacje, aby wyświetlić szczegółowe informacje o zainstalowanej wersji oprogramowania.

### 5.1 Licencja

W lewej części okna znajdziesz informację o czasie pozostałym do końca licencji na oprogramowanie G Data Software. Przed zakończeniem okresu licencyjnego otrzymasz automatyczne powiadomienie mailowe z propozycją wykupienia kontynuacji licencji przez Internet.

Na niedługo przed upłynięciem licencji na korzystanie z programu, program wyświetli komunikat o nadchodzącym terminie upływu ważności licencji.

Jeżeli chcesz dokonać przedłużenia licencji przez sklep internetowy, kliknij dymek z komunikatem, a następnie przycisk Zamów.

Jeśli produkt nie został aktywowany podczas instalacji, w sekcji Licencja dostępny jest Przycisk Aktywacja licencji.

---

Umożliwia wprowadzenie danych dostępu do aktualizacji lub zarejestrowanie nowej licencji.

Po dokonaniu aktywacji produktu, w sekcji Licencja dostępny jest przycisk Rozszerz licencję. Umożliwia wykupienie dodatkowych licencji w wygodny sposób przez stronę sklepu internetowego G Data.

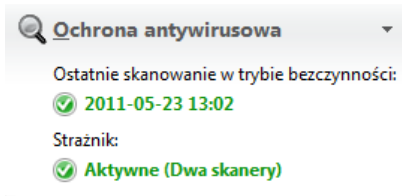
## **5.2 Obciążenie CPU**

Wykresy w sekcji Obciążenie CPU obrazują stopień obciążenia komputera. Wykres G Data pokazuje bieżące obciążenie procesora przez oprogramowanie G Data. Wykres System przedstawia sumaryczne obciążenie procesora przez wszystkie aplikacje. Podczas ręcznie uruchomionego skanowania komputera, obciążenie może być znaczące. Podczas normalnej pracy, program G Data obciąża system tylko w minimalnym stopniu, zapewniając maksymalną skuteczność ochrony.

Domyślnie program jest tak skonfigurowany, aby nie przeszkadzać w codziennej pracy. Skanowanie odbywa się wyłącznie wtedy, kiedy komputer jest w trybie bezczynności. Strażnik chroni komputer przez cały czas, niezależnie od zaplanowanych i ręcznie uruchamianych procesów skanowania.

## 6 Ochrona antywirusowa

Sekcja Ochrona antywirusowa informuje o stanie modułów skanujących. Umożliwia modyfikowanie ustawień związanych z działaniem monitora antywirusowego (Strażnika) i skanowaniem.



### Ostatnie skanowanie

Ten wiersz wyświetla datę ostatnio wykonanego skanowania komputera. Jeśli wiersz jest oznaczony czerwonym symbolem ostrzeżenia, zalecane jest ponowne przeprowadzenie skanowania. Kliknij wiersz z datą ostatniego skanowania, aby uruchomić skanowanie komputera. Po zakończeniu skanowania kolor wiersza zmieni się na zielony.

Szczegółowe informacje na temat skanowania znajdziesz w rozdziale: Co się dzieje podczas skanowania?

### Strażnik

Monitor antywirusowy powinien być zawsze włączony. Tylko wtedy program jest w stanie skutecznie uchronić komputer przed atakami wirusów.

---

Skanowanie i Strażnik: Obie funkcje pomagają chronić Twój komputer, mają jednak różne obszary zastosowania.

Strażnik służy do ciągłego monitorowania wszystkich zasobów komputera. Kontroluje wszystkie próby dostępu do plików. Powinien być zawsze włączony, gdyż jest to podstawowa składowa ochrony Twojego systemu.

Skanowanie stanowi uzupełnienie ochrony antywirusowej. Umożliwia przeskanowanie wszystkich lub wybranych zasobów komputera pod kątem infekcji. Dzięki tej funkcjonalności można wykryć wirusy, które mogły przeniknąć do komputera przed zainstalowaniem ochrony. Zalecane jest również w przypadku wykrycia wirusa przez Strażnika.

#### Menu sekcji Ochrona antywirusowa

Kliknij nagłówek sekcji Ochrona antywirusowa, aby rozwinąć menu umożliwiające wykonanie dodatkowych czynności.



**Skanuj komputer:** Polecenie uruchamia skanowanie wszystkich dysków lokalnych oraz obszarów systemowych. Szczegóły na temat skanowania znajdziesz w rozdziale: Co się dzieje podczas skanowania?



**Pamięć i autostart:** Program sprawdzi pliki oraz biblioteki DLL wszystkich bieżących procesów. Pozwoli to usunąć szkodliwe programy z pamięci (jeżeli nie od razu - zostaną wyeliminowane po kolejnym uruchomieniu komputera). W ten sposób zablokowana zostanie aktywność działających w systemie wirusów, bez potrzeby skanowania całego dysku. Zalecamy regularne przeprowadzanie profilaktycznego skanowania bieżących procesów i autostartu. Proces ten trwa o wiele krócej niż gruntowne skanowanie całego dysku twardego.



**Skanuj pliki/foldery:** To polecenie umożliwia przeskanowanie wybranych napędów, folderów i plików. Kliknij dwukrotnie tę pozycję aby otworzyć okno wyboru umożliwiające zaznaczenie elementów do przeskanowania.

Po lewej stronie okna wyboru znajduje się drzewo folderów rozwijanych przyciskiem +. Skontrolowany zostanie każdy obiekt zaznaczony

---

haczykiem. Jeśli nie zaznaczysz wszystkich podkatalogów czy plików danego katalogu, wiersz będzie koloru szarego. Czarnymi haczykami oznaczane są foldery skanowane w całości.



**Skanuj nośniki wymienne:** Ta funkcja służy do skanowania wymiennych napędów komputera, czyli płyt CD-ROM, DVD-ROM, dyskietek, kart pamięci Flash i pendrive'ów. Uruchomienie tej funkcji spowoduje przeskanowanie wszystkich nośników wymiennych widocznych w systemie. Pamiętaj, że programy nie mogą usuwać wirusów z nośników zabezpieczonych przed zapisem i płyt jednokrotnego zapisu. W przypadku wykrycia wirusa na takim nośniku, program może tylko sporządzić raport z wykrycia.



**Wykrywaj rootkity:** Użycie tego polecenia spowoduje uruchomienie narzędzia skanującego system na obecność rootkitów z pominięciem skanowania całego komputera.



**Wyłącz skanowanie w trybie bezczynności:** Strażnik przez cały czas obserwuje działanie systemu i kontroluje wszystkie próby dostępu do zasobów. Funkcja skanowania w trybie bezczynności uruchamia dodatkowo skaner

antywirusowy w momencie, kiedy system jest bezczynny. Skanowanie jest automatycznie przerywane, kiedy system przestaje być bezczynny.

Pomimo wyłączenia tej funkcji, komputer będzie nadal chroniony przez Strażnika.



**Wyłącz Strażnika:** Na życzenie użytkownika, skaner dostępowy (Strażnik) może zostać wyłączony. Zaleca się to jedynie w wyjątkowych i uzasadnionych przypadkach, np. na czas kopiowania dużych ilości danych lub wykonywania innych zasobożernych operacji (kopiowanie płyt DVD itp.). Po wykonaniu żądanych czynności należy niezwłocznie ponownie włączyć Strażnika. Podczas gdy Strażnik nie jest włączony, najlepiej nie nawiązywać połączenia z Internetem i nie podłączać niesprawdzonych pendrive'ów.



**Kwarantanna:** Kwarantanna to zaszyfrowany folder, w którym program przechowuje bezpiecznie zarażone pliki. Nie stanowią one w tej postaci zagrożenia dla systemu. Więcej szczegółów w rozdziale: Jak działa Kwarantanna?

---



Ustawienia: Ten przycisk otwiera okno ustawień programu z rozwiniętą listą ustawień ochrony antywirusowej. Szczegóły na temat ustawień znajdziesz w rozdziale: AntiVirus - Ustawienia

## 7 Sygnatury wirusów

Ta sekcja dostarcza informacji na temat aktualizacji sygnatur wirusów w programie G Data.

**Sygnatury wirusów**

Ostatnia aktualizacja:  
✔ 2011-05-24

Następna aktualizacja:  
✔ 41 min.

### Ostatnia aktualizacja

Ten wiersz wskazuje dokładny czas ostatniego przeprowadzenia aktualizacji sygnatur wirusów programu G Data. Jeśli wiersz wyróżniony jest czerwonym kolorem, przeprowadź jak najszybciej aktualizację sygnatur wirusów. W tym celu kliknij wiersz i wybierz polecenie Uaktualnij sygnatury wirusów.

### Następna aktualizacja

Ten wiersz wskazuje termin następnej zaplanowanej aktualizacji sygnatur wirusów.

Sygnatury wirusów: Programy antywirusowe wyposażone są w stale aktualizowane bazy cech, po których identyfikują zagrożenia. Jeśli plik lub program wykaże zgodność z wzorcem z bazy sygnatur programu G Data, zostanie natychmiast zakwalifikowany jako zagrożenie. Tylko regularna aktualizacja sygnatur wirusów zapewnia skuteczną ochronę przed zagrożeniami z Internetu.

### Menu sekcji Sygnatury wirusów

Kliknij nagłówek Sygnatury wirusów aby rozwinąć menu sekcji umożliwiające podjęcie dodatkowych działań:



**Uaktualnij sygnatury wirusów:** Sygnatury wirusów są pobierane automatycznie w godzinnych odstępach. Kliknij to polecenie, jeśli chcesz wymusić natychmiastowe pobranie najnowszych sygnatur wirusów.



**Wyłącz automatyczne aktualizacje:** Jeśli nie chcesz aby program automatycznie pobierał sygnatury wirusów, kliknij to polecenie. Wyłączenie automatu aktualizującego wzorce wirusów nie jest bezpieczne. Wyłączaj tę funkcję tylko w świadomie

---

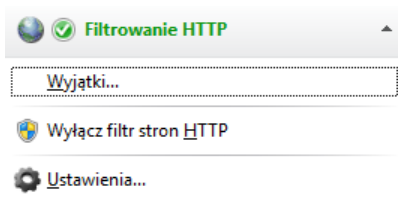
i w uzasadnionych przypadkach.



Ustawienia: To polecenie otwiera okno ustawień programu z rozwiniętą listą ustawień dotyczących aktualizacji programu. Więcej szczegółów na temat ustawień znajdziesz w rozdziale: AntiVirus - Ustawienia

## 8 Filtrowanie HTTP

Ta sekcja umożliwia włączanie/wyłączanie ochrony przeglądarek Internetowych. Filtr automatycznie weryfikuje otwierane strony pod kątem złośliwych programów i wyłudzenia informacji. Jeśli pobierana zawartość lub otwierana strona zostanie zakwalifikowana jako niebezpieczna, zagrożenie zostanie zgłoszone w postaci komunikatu, a strona nie otworzy się.



Jeśli spróbujesz pobrać niebezpieczny plik, program

G Data zatrzyma proces pobierania przed rozpoczęciem zapisu w folderze tymczasowych plików internetowych. W przeglądarce pojawi się odpowiedni komunikat.

Menu sekcji Filtrowanie HTTP

Kliknij nagłówek sekcji aby rozwinąć menu umożliwiające wykonanie dodatkowych czynności.

**Wyjątki:** W niektórych przypadkach, skanowanie HTTP może spowodować nieprawidłowe wyświetlanie danej strony Internetowej lub blokowanie usługi dostępnej przez stronę. Program umożliwia konfigurację wyjątków HTTP. Strony ustawione jako wyjątki nie są skanowane. Szczegóły na temat konfiguracji wyjątków HTTP znajdziesz w rozdziale: Wyjątki HTTP.

**Whitelist:** Lista bezpiecznych obiektów (np. stron internetowych) pomijanych w trakcie działania filtra HTTP.



**Wyłącz filtr stron HTTP:** Polecenie umożliwia wyłączenie ochrony przeglądarek. Może zaistnieć taka potrzeba, np. w przypadku pobierania dużych plików z zaufanych źródeł. Generalnie komputer jest chroniony przez inne warstwy ochrony pomimo wyłączenia ochrony w przeglądarce. Nie zalecamy jednak wyłączenia filtra HTTP na stałe,

ze względu na popularne ostatnio ataki stron wyłudzających informacje.



**Ustawienia:** To polecenie otwiera okno ustawień programu z rozwiniętą listą ustawień dotyczących ochrony przeglądarek. Więcej szczegółów na temat ustawień znajdziesz w rozdziale: Filtr HTTP - Ustawienia.

## **9 Ustawienia**

Przycisk Ustawienia otwiera okno umożliwiające dokonania modyfikacji w konfiguracji wszystkich składników pakietu. Opcje pogrupowane są w tematyczne grupy opisane w kolejnych rozdziałach. Domyślnie program jest ustawiony w sposób gwarantujący maksymalną ochronę. Modyfikowanie ustawień programu nie jest niezbędne.

### **9.1 AntiVirus - Ustawienia**

W tej sekcji znajdziesz ustawienia dotyczące ochrony przed wirusami.

### 9.1.1 Strażnik

Okno opcji Strażnika pozwala skonfigurować sposób monitorowania systemu plików przez Strażnika.

- **Status:** Opcja umożliwia całkowite wyłączenie monitora dostępowego (niezalecane).
  - **Skannery:** Strażnik może korzystać z dwóch niezależnych skanerów antywirusowych. Optymalną ochronę zapewnia zastosowanie dwóch skanerów. Praca skanerów jest skoordynowana w ten sposób, że minimalnie obciążają procesor. Jednak jeśli dysponujesz starszym sprzętem lub mniejszą ilością pamięci, spróbuj wyłączyć skaner dodatkowy. Wydajność pracy komputera na pewno wzrośnie. Sam skaner podstawowy również zapewnia skuteczną ochronę przed wirusami.
  - **Zarażone pliki:** Wybierz reakcję Strażnika na wykrycie wirusa. Automatyczne usuwanie wirusów wraz z plikami może doprowadzić do utraty ważnych danych lub plików systemowych. Jeśli nie chcesz korzystać z domyślnego ustawienia (Dialog z użytkownikiem), zastosowanie opcji Dezynfekcja (Jeśli niemożliwa: do Kwarantanny) umożliwia podjęcie decyzji o dalszych działaniach w późniejszym terminie.
  - **Zainfekowane archiwa:** Wybierz reakcję Strażnika na wykrycie wirusa w archiwach. Zalecamy wybranie opcji Dialog z użytkownikiem. Automatyczne usuwanie wirusów wraz z plikami może doprowadzić do utraty
-

skrzynek pocztowych lub ważnych danych.

Uwaga: Nie należy usuwać ani przenosić do Kwarantanny całych skrzynek pocztowych ani archiwów w przypadku wykrycia wirusa w jednej z wiadomości lub którymś pliku archiwum. Usunięcie pojedynczej wiadomości, można wykonać ręcznie w programie pocztowym.

- Ochrona rejestru: Jeżeli opcja Kontroli zachowania jest włączona, oprogramowanie pyta użytkownika o potwierdzenie każdej modyfikacji kluczowych ustawień rejestru lub plików systemowych np. przez instalowane aplikacje. Dzięki włączeniu tej opcji, złośliwe aplikacje nie są w stanie zmodyfikować treści pliku systemowego hosts bez wiedzy użytkownika. Mechanizm kontroli zachowania reaguje również, jeśli uruchomiona aplikacja zachowuje się podobnie jak złośliwe oprogramowanie.

W razie potrzeby można wyłączyć spod kontroli Strażnika wskazane napędy, foldery i pliki. Kliknij przycisk Wyjątki aby otworzyć okno wyjątków Strażnika. Aby dodać nowy wyjątek kliknij przycisk Nowy. Wskaż rodzaj obiektu, który chcesz pomijać przy kontroli (napęd, folder lub plik). Przycisk ... otworzy okno wyboru katalogu lub napędu.

Aby utworzyć wyjątek, wykonaj następujące kroki:

- 1 Kliknij przycisk Wyjątki.

- 2 W oknie wyjątków kliknij przycisk Nowy:
- 3 Wybierz rodzaj wyjątku. Można tworzyć wyjątki dla napędów, folderów lub plików.
- 4 W oknie wyboru wskaż obiekt, który chcesz wyjąć spod ochrony Strażnika. Jeżeli tworzysz wyjątek dla pliku, wpisz ręcznie jego nazwę lub zastosuj maskę pliku używając znaków zastępczych.

Dozwolone jest stosowanie następujących znaków zastępczych.

? Symbolizuje dowolny znak.

\* Zastępuje dowolny ciąg znaków.

Przykładowo wykluczenie wszystkich plików z rozszerzeniem exe można zdefiniować stosując maskę pliku \*.exe. Wyjątki dla różnych plików arkuszy kalkulacyjnych (xlr i xls) można ustawić wpisując tekst \*.xl?. Jeżeli nie chcesz, żeby Strażnik skanował pliki, których nazwy rozpoczynają się od konkretnego słowa, np. tekst, wprowadź maskę tekst\*.\*.

---

5 Kliknij przycisk OK. Wyjątek pojawi się na liście.

6 Kliknij OK, aby zamknąć okno wyjątków.

Proces można powtarzać wielokrotnie. Można również usuwać i modyfikować zdefiniowane obiekty wyjątków.

Kliknij przycisk Zaawansowane, aby otworzyć okno zaawansowanych ustawień Strażnika.

- Tryb: Domyślnie Strażnik skanuje pliki zarówno podczas odczytu jak i zapisu. Jest to najbezpieczniejsza opcja. Na żądanie można ograniczyć Strażnika do weryfikowania jedynie podczas odczytywania, lub jedynie podczas uruchamiania plików.
- Skanuj zasoby sieciowe: Jeśli komputer jest połączony w sieci z innymi stanowiskami, nie chronionymi przez program antywirusowy, (np. notebook), warto uruchomić opcje kontroli zasobów sieciowych. Strażnik będzie kontrolował zapis i odczyt plików znajdujących się na podłączonych w sieci komputerach. Nie musisz uruchamiać tej opcji, jeżeli Twój komputer nie jest połączony z innymi lub też jeżeli na podłączonych do sieci innych komputerach zainstalowana jest ochrona przed wirusami.
- Heurystyka: Analiza heurystyczna różni się od zwykłego skanowania tym, że nie tylko wynajduje

wirusy porównując pliki z sygnaturami wirusów, ale rozpoznaje je po typowych cechach spotykanych u tego typu programów. Ta metoda, choć wzmacnia skuteczność wykrywania wirusów, jest jednak bardzo czasochłonna. W niektórych przypadkach może także powodować fałszywe alarmy.

- Skanuj archiwa: Skanowanie plików spakowanych trwa bardzo długo i nie jest potrzebne jeśli Strażnik jest włączony. Strażnik wychwytuje wirusy w chwili rozpakowywania archiwów i zapobiega ich dalszemu rozprzestrzenianiu się.
  - Skanuj pliki e-mail: Program kontroluje pocztę elektroniczną za pomocą modułu POP3 dla Outlook Express i podobnych oraz wtyczki do programu MS Outlook, nie ma więc potrzeby używania tej opcji.
  - Skanuj obszary systemowe przy starcie komputera: Obszary systemowe (boot sektor, Master Boot Record itd.) stanowią niezwykle ważny element każdego systemu operacyjnego.
  - Skanuj obszary systemowe przy zmianie nośnika: Obszary systemowe powinny być kontrolowane przy każdej sposobności. Ta opcja uruchomi skanowanie sektorów startowych przy każdej zmianie nośnika (np. włożenie do napędu nowej płytki CD-ROM).
  - Wykrywaj dialery/spyware/adware/riskware: To ustawienie włącza moduł wykrywający dialery, a także programy podwyższonego ryzyka, których stosowanie
-

może obniżyć poziom bezpieczeństwa systemu.

- Skanuj tylko nowe i zmodyfikowane pliki: Skanuj tylko nowe i zmodyfikowane pliki: Włączenie tej opcji spowoduje pomijanie podczas skanowania plików, które zostały już wcześniej sprawdzone i zakwalifikowane jako bezpieczne. Jeżeli dany plik uległ modyfikacji, zostanie sprawdzony pomimo włączenia tej opcji..

## **9.1.2 Ręczne skanowanie**

Okno opcji skanowania pozwala dopasować parametry skanowania danych. Najlepiej przeprowadzać skanowanie komputera w chwili, kiedy nie jest obciążony innymi zadaniami. Umożliwi to wykorzystanie do skanowania wszystkich zasobów systemowych komputera, a tym samym nie będzie przeszkadzać użytkownikowi w pracy.

Do dyspozycji są następujące opcje i parametry:

- Skanery: Program korzysta z dwóch niezależnych skanerów antywirusowych. Optymalne efekty daje zastosowanie obu skanerów. Przy użyciu tylko jednego z nich, proces sprawdzania trwa krócej, ale jest mniej dokładny. Zalecamy ustawienie Dwa skanery. Praca skanerów jest skoordynowana w ten sposób, że minimalnie obciąża procesor.
- Zarażone pliki: Wybierz reakcję skanera na wykrycie wirusa. Zalecamy wybranie opcji Dezynfekcja (Jeśli

niemożliwa: zablokuj dostęp do pliku). Automatyczne usuwanie wirusów wraz z plikami może doprowadzić do utraty ważnych danych lub plików systemowych. Zastosowanie opcji Dezynfekcja (Jeśli niemożliwa: przenieś do Kwarantanny) umożliwia podjęcie decyzji o dalszych działaniach w późniejszym terminie.

- **Zainfekowane archiwa:** Wybierz reakcję skanera na wykrycie wirusa w archiwach. Wirusy w plikach archiwalnych mogą stanowić zagrożenie dopiero w momencie rozpakowania archiwum. Strażnik wykryje i zablokuje wirusa w momencie uruchomienia dekompresji. Skanowanie archiwów zalecane jest przed przekazaniem lub przesłaniem spakowanych plików innym użytkownikom, jeżeli nie masz pewności, że stosują skuteczne oprogramowanie antywirusowe.
- **Wstrzymaj skanowanie na czas aktywności systemu:** Ta funkcja spowoduje wstrzymanie skanowanie w momencie przeprowadzania przez system operacyjny innych działań. Skanowanie zostanie automatycznie wznowione w momencie, kiedy komputer znów będzie beczynny.

Wyjątki...

Kliknij ten przycisk, jeśli chcesz ustawić foldery i pliki wykluczeń. Te obiekty nie będą skanowane:

1. Kliknij przycisk Wyjątki.
-

2. Kliknij przycisk Nowy...
3. Wybierz rodzaj wyjątku.
4. Wskaż napęd, wybierz foldery lub wpisz maskę pliku stosując znaki zastępcze.

Dozwolone są następujące znaki zastępcze:

- Znak zapytania (?) zastępuje dowolny znak.
- Gwiazdka (\*) zastępuje dowolny ciąg znaków.

Aby pomijać przy skanowaniu wszystkie pliki z rozszerzeniem .sav wpisz maskę \*.sav. Aby pomijać pliki o nazwach tekst1.doc, tekst2.doc, tekst3.doc), wpisz maskę tekst?.doc.

Kliknij przycisk Zaawansowane, aby otworzyć okno zaawansowanych ustawień skanowania:

- Rodzaje plików: Strażnik może skanować wszystkie pliki, lub tylko pliki programowe i dokumenty.
- Heurystyka: Analiza heurystyczna różni się od zwykłego skanowania tym, że nie tylko wynajduje

wirusy porównując pliki z sygnaturami wirusów, ale rozpoznaje je po typowych cechach spotykanych u tego typu programów. Ta metoda, choć wzmacnia skuteczność wykrywania wirusów, jest jednak bardzo czasochłonna. W niektórych przypadkach może także powodować fałszywe alarmy.

- Skanuj archiwa: Skanowanie plików spakowanych trwa bardzo długo i nie jest potrzebne jeśli Strażnik jest włączony. Strażnik wychwytuje wirusy w chwili rozpakowywania archiwów i zapobiega ich dalszemu rozprzestrzenianiu się.
  - Skanuj pliki e-mail: Program kontroluje pocztę elektroniczną za pomocą modułu POP3 dla Outlook Express i podobnych oraz wtyczki do programu MS Outlook, nie ma więc potrzeby używania tej opcji.
  - Skanuj obszary systemowe: Obszary systemowe (boot sektor, Master Boot Record itd.) stanowią podstawę systemu operacyjnego, zaleca się skanowanie obszarów systemowych co jakiś czas.
  - Wykrywaj dialery/spyware/adware/riskware: To ustawienie włącza moduł wykrywający dialery, a także programy podwyższonego ryzyka, których stosowanie może obniżyć poziom bezpieczeństwa systemu.
  - Wykrywaj rootkity: Opcja włącza dodatkowy skaner wykrywający rootkity, czyli mechanizmy służące do ukrywania złośliwych programów przed oprogramowaniem zabezpieczającym.
-

- Skanuj tylko nowe i zmodyfikowane pliki: Włączenie tej opcji spowoduje pomijanie podczas skanowania plików, które zostały już wcześniej sprawdzone i zakwalifikowane jako bezpieczne. Jeżeli dany plik uległ modyfikacji, zostanie sprawdzony pomimo włączenia tej opcji.
- Twórz raport: Jeśli zaznaczysz pole Twórz raport, program będzie protokołował każdy proces skanowania.

## **10 Warto wiedzieć**

Ten rozdział zawiera kilka porad związanych z obsługą programu G Data Security.

### **10.1 Instalacja pełna czy niestandardowa?**

Wybranie pełnej instalacji spowoduje zainstalowanie składników zalecanych dla większości użytkowników. Jeśli chcesz samodzielnie wybrać składniki do instalacji, wybierz instalację niestandardową.

Program umożliwia zmodyfikowanie składu instalacji także po zakończeniu instalacji. W tym celu wystarczy rozpocząć instalację ponownie i zaznaczyć pożądane

składniki. Nie jest konieczne usuwanie całego pakietu i instalowanie go od nowa.

### 10.2 Płyta startowa

Dzięki płycie startowej można przeprowadzić skanowanie lokalnych napędów, wykazujące ewentualną obecność wirusa lub rootkita na dysku lub w pamięci. Skanowanie odbywa się bez udziału systemu Windows.

Płyta startowa umożliwia również przywrócenie partycji lub dysku, jeśli wcześniej sporządzona została kopia zapasowa (dostępne w pakietach G Data TotalCare i G Data NotebookSecurity).

W celu rozpoczęcia skanowania uruchom komputer z oryginalnej płyty z oprogramowaniem G Data Software lub z płyty startowej sporządzonej przy pomocy programu G Data.

Upewnij się, że komputer automatycznie startuje z płyty CD-ROM. Jeśli nie, zmień kolejność uruchamiania urządzeń w menu BIOS. Jako pierwsze urządzenie bootujące (1st Boot Device) należy ustawić napęd CD-ROM, dysk twardy z systemem operacyjnym jako drugie (2nd Boot Device). Jeżeli płyta startowa znajduje się w napędzie, uruchomiona zostanie wersja programu oparta o system Linux. Jeżeli płyty nie ma w napędzie, komputer uruchomi automatycznie system Windows z dysku twardego.

---

Wskazówka: Niektóre płyty główne umożliwiają zmianę kolejności uruchamiania urządzeń po wciśnięciu klawisza F11, F8 lub F2. W przypadku wątpliwości dotyczących sposobu zmiany kolejności uruchamiania, zapoznaj się z dokumentacją dołączoną do płyty głównej. Po przeprowadzeniu skanowania wstępnego i zainstalowaniu programu, zaleca się przywrócenie pierwotnej kolejności uruchamiania.

1. Włóż płytę startową do napędu CD/DVD. Uruchom komputer ponownie. Komputer sam odnajdzie na i uruchomi moduł płyty startowej. Wybierz z wyświetlonego menu pożądaną metodę uruchomienia płyty startowej:

- Microsoft Windows: Jeżeli nie chcesz uruchamiać modułu skanującego, wybierz tę opcję aby uruchomić Twój system operacyjny Windows.
- Płyta startowa G Data: To polecenie uruchamia moduł płyty startowej w standardowym trybie graficznym.
- Płyta startowa G Data - tryb bezpieczny: Jeżeli standardowy moduł płyty startowej powoduje problemy z wyświetlaniem, lub Twój komputer nie obsługuje prawidłowo modułu płyty startowej, możesz wybrać uproszczony moduł płyty startowej pracujący w trybie tekstowym.

2. Wybierz pożądaną opcję przy pomocy klawiszy strzałek i wciśnij przycisk Enter.

3. Płyta startowa uruchomi się system operacyjny Linux z

wbudowanym oprogramowaniem G Data Software działającym bez udziału systemu operacyjnego Windows.

4. Przeprowadź skanowanie komputera i usuń wszystkie wykryte wirusy używając opcji oferowanych przez program.

6. Uruchom komputer ponownie wybierając opcję Microsoft Windows, aby uruchomił się Twój system operacyjny.

Skanowanie wstępne przy użyciu płyty startowej to najskuteczniejsze narzędzie do wykrywania rootkitów uruchomionych w systemie.

### 10.3 Ikona paska zadań

Ikona programu znajduje się w zasobniku systemowym, czyli w prawym, dolnym rogu ekranu (obok zegarka).



Tak wygląda ikona, jeżeli wszystkie niezbędne funkcje programu są włączone.



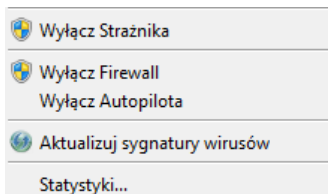
Jeżeli któryś z kluczowych składników ochrony jest wyłączony lub nie działa prawidłowo na ikonce pojawia się znak ostrzeżenia.

---



Wygląd ikony podczas pobierania aktualizacji.

Dwukrotne kliknięcie ikony powoduje uruchomienie interfejsu programu. Klikając ikonę prawym klawiszem myszy otworzysz menu kontekstowe zawierające kilka podstawowych poleceń.



Menu umożliwia między innymi wyłączenie Strażnika na określony czas. Polecenie Aktualizuj sygnatury wirusów pozwala pobrać najnowsze sygnatury wirusów bez potrzeby uruchamiania okna programu. Z tego miejsca możesz również przejrzeć Statystyki dotyczące wykrytych wirusów, przeskanowanych wiadomości pocztowych i stron internetowych.

Jeśli Twoje oprogramowanie wyposażone jest w składnik Firewall, w menu ikony widnieją dodatkowo polecenia Wyłącz Firewall i Wyłącz autopilota.

Polecenie Wyłącz Firewall pozwala na czasowe wyłączenie zapory sieciowej. Po wyłączeniu zapory komputer nie jest

chroniony przed atakami z Internetu. Przy pomocy tej opcji można wyłączyć zaporę maksymalnie do ponownego uruchomienia komputera.

Kliknięcie polecenia Wyłącz autopilota wyłącza mechanizm, który automatycznie zezwala aplikacjom na łączenie się z Internetem. Zapora przełączy się w tryb ręczny i przestanie automatycznie zezwalać programom na łączenie się z internetem.

## **10.4 Co to są aktualizacje sygnatur wirusów?**

Aktualizowanie sygnatur wirusów polega na pobieraniu najnowszej wersji bazy znanych wirusów z serwera aktualizacji do programu antywirusowego. Dzięki regularnie przeprowadzanym aktualizacjom program uczy się rozpoznawać najnowsze szkodliwe programy.

Pracownicy G Data SecurityLabs na bieżąco opracowują najnowsze sygnatury wirusów i przygotowują aktualizacje programu. Z efektów ich pracy korzystasz na co dzień - pobierając uaktualnienia uczące Twój program rozpoznawania najnowszych zagrożeń.

---

## **10.5 Co to jest aktualizacja oprogramowania?**

Podobnie jak sygnatury wirusów, można uaktualnić również pozostałe elementy oprogramowania G Data. Do tego służy opcja aktualizacji plików programu.

Uaktualnianie oprogramowania to praktyka stosowana przez wszystkich producentów programów komputerowych. Umożliwia usprawnianie programów, modyfikowanie ich wyglądu, a także poprawianie zawartych w nich błędów.

## **10.6 Jak uaktualnić sygnatury wirusów?**

Istnieje kilka sposobów na uaktualnienie sygnatur wirusów.

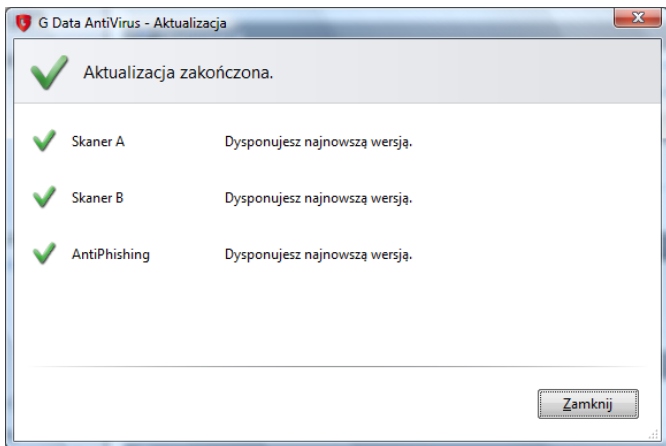
- **Wymuszenie ręcznej aktualizacji:** W głównym oknie programu kliknij nagłówek sekcji Sygnatury wirusów i wybierz polecenie Uaktualnij sygnatury wirusów. Program sam pobierze i zainstaluje pliki zawierające definicje najnowszych wirusów.
- **Automatyczne aktualizowanie sygnatur wirusów:** Po zainstalowaniu programu, aktualizacje automatyczne są domyślnie włączone. Jeśli są wyłączone, w wierszu Automatyczne aktualizacje w sekcji Aktualizacje pojawi się czerwony znak ostrzeżenia. Sposób konfigurowania aktualizacji automatycznych opisany jest w rozdziale Aktualizacje.

## 40 G Data Security

---

- Program informuje, że aktualizacja nie została przeprowadzona od dłuższego czasu: Kliknij przycisk Napraw w górnej części okna aby uruchomić aktualizację.

W trakcie przeprowadzania ręcznej aktualizacji otwiera się okno, w którym można śledzić postęp aktualizowania poszczególnych składników programu.



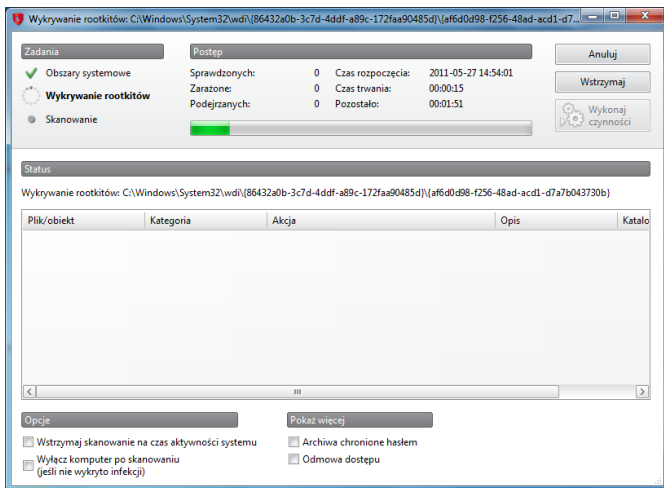
Do przeprowadzenia aktualizacji niezbędne jest połączenie z Internetem.

---

## 10.7 Skanowanie

Skanowanie polega na porównywaniu wszystkich plików objętych skanowaniem z wzorcami wirusów (sygnaturami), którymi dysponuje program antywirusowy. Jeżeli program wykryje w pliku zgodność z jedną z sygnatur, zarejestruje ten fakt jako wykrycie wirusa.

W trakcie trwania skanowania wyświetlone jest okno skanowania.



W górnej części okna, w sekcji Postęp wyświetlane są statystyki dotyczące procesu skanowania. Pasek postępu wskazuje procent wykonania skanowania komputera. W sekcji status wyświetlana jest ścieżka dostępu oraz nazwa skanowanego w danym momencie pliku. Środkowa część okna przedstawia wyniki skanowania oraz wykryte zagrożenia. Już w tym miejscu masz możliwość podjęcia decyzji, jak postąpić z wykrytymi zagrożeniami.

Przycisk Anuluj umożliwia przerwanie skanowania w dowolnym momencie. Użycie przycisku Wstrzymaj powoduje tymczasowe wstrzymanie skanowania i pozwala na wznowienie skanowania w dowolnym momencie.

Zaznaczenie opcji Wstrzymaj skanowanie na czas aktywności systemu spowoduje wstrzymanie skanowanie w momencie wykonywania przez system innych działań. Skanowanie zostanie wznowione w momencie, kiedy komputer znów będzie bezczynny.

Opcja Wyłącz komputer po skanowaniu spowoduje wyłączenie komputera, jeśli skanowanie nie wykryje niebezpiecznych plików.

W sekcji Pokaż więcej możesz zdecydować czy chcesz także oglądać wyniki skanowania dotyczące archiwów, plików, do których program nie ma dostępu i archiwów zabezpieczonych hasłem.

W przypadku wykrycia wirusa program odnotuje ten fakt na liście w oknie skanowania. Po zakończeniu skanowania, można ustalić co program ma zrobić z

---

danym zagrożeniem. Kliknij pole w kolumnie Akcja i wybierz z listy rozwijanej czynność, którą chcesz wykonać. Można ustalić inną akcję dla każdego wykrytego zagrożenia. Po dokonaniu wyboru kliknij przycisk Wykonaj czynności.

Po wykonaniu wybranych czynności odblokuje się przycisk Zamknij. Kliknij go, aby zamknąć okno skanowania.

## **10.8 Wykrycie wirusa**

W przypadku wykrycia wirusa program wyświetla okno zawierające nazwę wirusa, a także lokalizację i nazwę pliku z wykrytym wirusem.

Okno umożliwia podjęcie wybranego działania. W większości przypadków najlepszym rozwiązaniem jest wybranie opcje Przenieś do Kwarantanny). Plik z wirusem zostanie przeniesiony do zaszyfrowanego folderu Kwarantanny. Bezpośrednie usuwanie całego pliku z wirusem może spowodować usunięcie ważnego pliku systemowego lub istotnych danych. Wybranie opcji Zablokuj dostęp do pliku spowoduje że program uniemożliwi uruchamianie i kopiowanie pliku.

### Kwarantanna i skrzynki pocztowe

Nie zaleca się przenoszenia do Kwarantanny plików programów pocztowych zawierających całe skrzynki pocztowe (np \*.PST, \*.DBX). Po przeniesieniu plików poczty do Kwarantanny program pocztowy nie odnajdzie ich w domyślnych lokalizacjach i nie będzie w stanie wyświetlić pobranych wcześniej wiadomości, lub też przestanie działać prawidłowo.

## 10.9 Inicjatywa G Data Malware Information

Co to jest Inicjatywa G Data Malware Information?

Specjaliści G Data Security Labs rozwijają mechanizmy chroniące Klientów G Data przed złośliwym oprogramowaniem. Skuteczność działania i szybkość tworzenia mechanizmów ochronnych zależy w dużej mierze od posiadanych informacji na temat złośliwego oprogramowania. Informacje na temat szkodliwych programów najlepiej pozyskiwać bezpośrednio z zaatakowanych lub zainfekowanych komputerów. Inicjatywa G Data Malware Information umożliwia przekazywanie informacji na temat zagrożeń. Dzięki przystąpieniu do Inicjatywy, możesz wspomóc zespół specjalistów G Data Security Labs wysyłając informacje o złośliwych programach atakujących Twój komputer. Twój udział w Inicjatywie G Data Malware Information wpłynie bezpośrednio na podniesienie jakości produktów

---

oferowanych przez G Data Software.

Jakie dane zbieramy?

Informacje gromadzone są na dwa sposoby:

1. Użytkownik samodzielnie wysyła szkodliwe oprogramowanie przy pomocy opcji wysyłki plików do Ambulansu G Data. W tym przypadku, wraz z plikami przekazywane są ich oryginalne nazwy, lokalizacje w systemie i daty utworzenia.
2. Automatyczna wysyłka złośliwych plików wykrytych na odwiedzanych stronach internetowych. Do G Data Security Labs wysyłane są następujące informacje:
  - Wersja Malware Information
  - Numer wersji produktu G Data i używane skanery
  - Język systemu operacyjnego
  - Adres URL do zablokowanej strony, zawierającej złośliwy kod (malware, phishing itd.)
  - Nazwa złośliwego programu

Przesyłane dane nie służą identyfikacji użytkowników zarażonych komputerów. Informacje nie są zestawiane z danymi osobowymi.

W jaki sposób wykorzystujemy dane?

Przechowywanie i obróbka danych odbywa się z poszanowaniem norm dotyczących ochrony danych osobowych, obowiązujących we wszystkich krajach. Szczególny nacisk kładziemy na zabezpieczanie danych przed dostępem osób nieuprawnionych.

Analizowanie danych ma miejsce w pomieszczeniach G Data Security Labs i służy tylko badaniom i wyjaśnianiu zagadnień z zakresu bezpieczeństwa IT. Celem badań jest określenie potencjalnych zagrożeń i rozwijanie mechanizmów ochronnych. Przykładowo, na podstawie przesyłanych danych tworzone są listy blokowanych stron, statystyki na potrzeby publikacji w fachowej prasie, czy też zestawy reguł stosowane w technologiach zabezpieczających. Udział w Inicjatywie jest dobrowolny, a odmowa udziału nie ma negatywnego wpływu na skuteczność działania produktu G Data. Pamiętaj, że Twój udział w Inicjatywie G Data Malware Information podnosi świadomość zagrożeni, a także skuteczność zabezpieczeń oprogramowania zainstalowanego u wszystkich użytkowników G Data.

### **10.10 Komunikat "not-a-virus"**

W ten sposób oznaczane są pliki programów, które choć nie są wirusami, stanowią teoretyczne zagrożenie dla komputera. Same w sobie nie są groźne, ale ich stosowanie może ułatwić przeprowadzenie ataku na

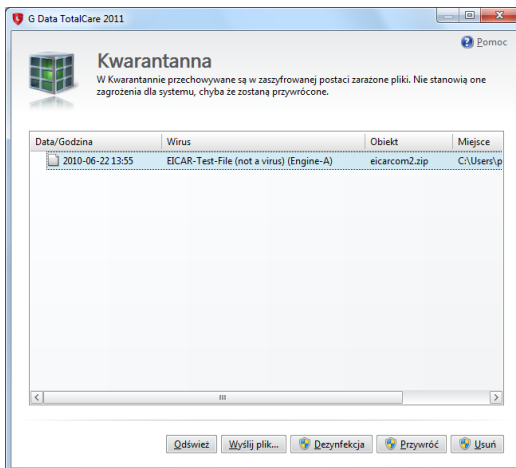
---

komputer. Do takich programów należą między innymi aplikacje do zdalnego zarządzania komputerami przy pomocy protokołu VNC (RealVNC, TightVNC), aplikacje do korzystania z komunikacji IRC, serwery FTP.

Jeżeli są to świadomie używane aplikacje, nie zalecamy usuwania takich plików, ani przenoszenia ich do Kwarantanny, gdyż spowoduje to, że przestaną one funkcjonować poprawnie.

## 10.11 Kwarantanna

Kwarantanna to zaszyfrowany folder, w którym program przechowuje bezpiecznie zarażone pliki. Nie stanowią one w tej postaci zagrożenia dla systemu. Decyzję, co zrobić z zarażonymi plikami, można w ten sposób odłożyć na później. Zaznacz wybrany plik w folderze Kwarantanny i zdecyduj, czy chcesz go zdezynfekować, przywrócić czy też usunąć.



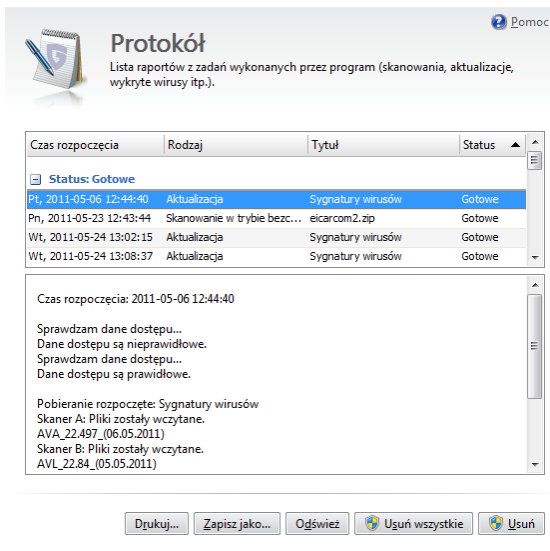
- **Dezynfekcja:** Jeżeli wirus nie zniszczył zarażonego pliku, program może usunąć kod wirusa i odzyskać dane w oryginalnej postaci. Odzyskane pliki
-

przenoszone są automatycznie do folderu źródłowego.

- **Przywróć:** Czasem zachodzi konieczność przywrócenia pliku do pierwotnej lokalizacji, pomimo, że nie da się go zdezynfekować gdyż wirus uszkodził jego część. Jeżeli zajdzie potrzeba przywrócenia zarażonego pliku, zaleca się zachowanie wszelkich możliwych środków ostrożności (odłączenie komputera od sieci lokalnej/Internetu, sporządzenie kopii zapasowych ważnych, niezarażonych danych).
- **Wyślij plik:** Istnieje możliwość przesłania zarażonego pliku z Kwarantanny do Ambulansu G Data. Możesz to zrobić, jeśli masz skonfigurowane konto e-mail w programie pocztowym. Patrz też rozdział: Inicjatywa G Data Malware Infomation.
- **Usuń:** Jeżeli plik nie jest potrzebny, można go po prostu usunąć z Kwarantanny.

## 10.12 Raporty

Widok raportów zawiera listę wszystkich raportów z działań programu. Klikając nagłówki poszczególnych kolumn, możesz posortować je według czasu rozpoczęcia, rodzaju, tytułu lub statusu. Dostęp do okna raportów jest też możliwy poprzez ikonkę Raporty w górnej części okna głównego.



**Protokół** Pomoc

Lista raportów z zadań wykonanych przez program (skanowania, aktualizacje, wykryte wirusy itp.).

Czas rozpoczęcia	Rodzaj	Tytuł	Status
[-] Status: Gotowe			
Pt, 2011-05-06 12:44:40	Aktualizacja	Sygnatury wirusów	Gotowe
Pn, 2011-05-23 12:43:44	Skanowanie w trybie bezc...	eicarcom2.zip	Gotowe
Wt, 2011-05-24 13:02:15	Aktualizacja	Sygnatury wirusów	Gotowe
Wt, 2011-05-24 13:08:37	Aktualizacja	Sygnatury wirusów	Gotowe

Czas rozpoczęcia: 2011-05-06 12:44:40

Sprawdzam dane dostępu...  
Dane dostępu są nieprawidłowe.  
Sprawdzam dane dostępu...  
Dane dostępu są prawidłowe.

Pobieranie rozpoczęte: Sygnatury wirusów  
Skaner A: Pliki zostały wczytane.  
AVA\_22.497\_(06.05.2011)  
Skaner B: Pliki zostały wczytane.  
AVL\_22.84\_(05.05.2011)

Drukuj... Zapisz jako... Odśwież Usuń wszystkie Usuń

Aby obejrzeć raport, zaznacz jego wiersz. Zawartość raportu pojawi się w dolnej części okna. Istnieje możliwość wydrukowania lub zapisania protokołu do pliku za pomocą przycisków Zapisz jako... i Drukuj.... Dostępne formaty to ASCII (txt) oraz HTML.

Aby usunąć raport, zaznacz jego nazwę i kliknij przycisk Usuń. Przycisk Usuń wszystkie spowoduje wyczyszczenie listy raportów.

## **10.13 Licencje wielostanowiskowe**

Licencje wielostanowiskowe umożliwiają korzystanie z jednej licencji na większej ilości komputerów. Rejestracja odbywa się tylko raz - na pierwszym komputerze. Na pozostałych stanowiskach należy wpisać dane dostępu uzyskane w potwierdzeniu rejestracji.

Do czego służy numer rejestracyjny?

Numer rejestracyjny służy do zarejestrowania licencji w celu uzyskania danych dostępu do aktualizacji (Użytkownik i Hasło). Rejestracja danego numeru rejestracyjnego może odbyć się tylko raz.

Dlaczego podczas rejestracji pojawia się komunikat:  
Produkt został już zarejestrowany?

Rejestracji można dokonać tylko raz. Na każdym kolejnym komputerze wystarczy wpisać dane dostępu otrzymane w potwierdzeniu pierwszej rejestracji.

Nie da się zarejestrować danego numeru po raz drugi. Wpisz dane dostępu i kliknij OK, bez otwierania okna Rejestracja online. W razie problemów, skontaktuj się z pomocą techniczną G Data.

## **10.14 Kontynuacja licencji**

Na niedługo przed upłynięciem licencji na korzystanie z programu, ikonka w zasobniku systemowym pokazuje komunikat o nadchodzącym terminie upływu ważności licencji.

Kliknij dymek, jeżeli chcesz dokonać przedłużenia licencji przez sklep internetowy. Jeśli chcesz zostać przeniesiony na stronę internetową sklepu, kliknij przycisk Zamów.

Jeśli chcesz wcześniej dokonać przedłużenia lub rozszerzenia licencji na większą ilość stanowisk, skontaktuj się ze sprzedawcą lub skorzystaj ze sklepu internetowego G Data klikając przycisk Rozszerz licencję... w lewej części okna programu G Data Security.

## **10.15 Przeniesienie licencji na inny komputer**

Po prostu odinstaluj program z jednego komputera i zainstaluj na drugim. Przy próbie aktualizacji program sam zapyta, czy przenieść licencję. Po przeniesieniu licencji poprzedni komputer utraci możliwość pobierania aktualizacji.

---

## 10.16 Deinstalacja programu

Najprostszą metodą usunięcia programu z systemu jest skorzystanie z polecenia Usun w grupie programowej G Data menu Start systemu Windows. Sam proces instalacji przebiega automatycznie.

Alternatywną metodą jest deinstalacja poprzez Panel sterowania systemu Windows.

- Windows XP: Uruchom polecenie menu Start > Panel sterowania. W Panelu sterowania otwórz aplet Dodaj/Usun programy. Znajdź na liście nazwę zainstalowanego produktu G Data Software, zaznacz ją myszką i kliknij przycisk Usun.
- Windows Vista, 7: Uruchom polecenie menu Start > Panel sterowania. W Panelu sterowania otwórz aplet Programy i funkcje. Znajdź na liście nazwę zainstalowanego produktu G Data Software, kliknij ją prawym klawiszem myszki i wybierz polecenie Usun.

Podczas instalacji program zapyta, czy usunac ustawienia i raporty programu. Jezeli zamierzasz zainstalowac nowsza wersje programu, pozwol na usuniecie tych elementow.

Jeśli w Kwarantannie programu znajdują się zarażone pliki, program zapyta podczas deinstalacji, czy chcesz je usunac. Jezeli ich nie usuniesz, beda dostepne w Kwarantannie po zainstalowaniu nowszej wersji programu G Data.

## **11 Warunki licencji**

Ogólne warunki licencji użytkowania oprogramowania G Data Security.

1. Przedmiot umowy. Przedmiotem umowy zawartej między firmą G Data Software Sp. z o.o., zwaną dalej Producentem, a Użytkownikiem jest oprogramowanie zabezpieczające firmy G Data Software zwane dalej Oprogramowaniem. Producent dostarcza Użytkownikowi Oprogramowanie na nośniku danych lub w postaci pliku pobranego ze strony internetowej Producenta. Producent zwraca uwagę na fakt, że technicznie nie jest możliwe wyprodukowanie Oprogramowania współpracującego bezbłędnie z wszystkimi aplikacjami i z każdą kombinacją sprzętowo-programową.
  2. Zakres stosowania Użytkownik otrzymuje proste, niewyłączne i osobiste prawo, zwane dalej Licencją, do używania Oprogramowania na każdym kompatybilnym komputerze pod warunkiem, że Oprogramowanie będzie użytkowane na nie większej niż uzgodniona z Producentem ilości komputerów, maszyn wirtualnych lub sesji terminali. Jeżeli z komputera korzysta więcej niż jedna osoba, Licencja obejmuje wszystkie osoby korzystające z komputera. Użytkownik ma prawo przenieść Oprogramowania z jednego komputera na drugi, przy zachowaniu uzgodnionej z Producentem maksymalnej ilości komputerów.
-

- 
3. Szczególne ograniczenia Użytkownik nie może modyfikować Oprogramowania bez pisemnej zgody Producenta.
  4. Prawo własności Zakupując Oprogramowanie Użytkownik nabywa prawo własności do nośnika z zapisanym Oprogramowaniem, a także czasowe prawo do otrzymywania aktualizacji i pomocy technicznej. Zakup Oprogramowania nie wiąże się z zakupem praw do Oprogramowania. Producent zastrzega sobie w szczególności wszystkie prawa do publikowania, powielania, modyfikacji i eksploatacji Oprogramowania.
  5. Powielanie Oprogramowanie i dokumentacja pisemna chronione są prawem autorskim. Dozwolone jest sporządzenie jednej kopii bezpieczeństwa Oprogramowania; kopia nie może zostać przekazana osobom trzecim.
  6. Czas trwania umowy Umowa zostaje zawarta na czas nieokreślony. Czas trwania umowy nie obejmuje prawa do otrzymywania aktualizacji i pomocy technicznej. Prawo do użytkowania Oprogramowania wygasa automatycznie bez okresu wypowiedzenia w momencie złamania przez Użytkownika któregokolwiek z postanowień tej umowy. Wraz z wygaśnięciem umowy Użytkownik jest zobowiązany do zniszczenia oryginalnego nośnika z Oprogramowaniem oraz dokumentacji pisemnej.
  7. Złamanie warunków umowy Użytkownik ponosi

odpowiedzialność za wszystkie szkody poniesione przez Producenta w związku z naruszeniem praw autorskich, wynikłe ze złamania warunków tej umowy.

8. Gwarancja i odpowiedzialność Producenta:

- a. Producent gwarantuje, że w momencie przekazania Oprogramowania pierwotnemu Użytkownikowi, jest ono pozbawione błędów i zdadne do użytku w myśl dołączonej specyfikacji programu.
  - b. W przypadku stwierdzenia wady nośnika lub pobranego pliku, Użytkownik zobowiązany jest do zgłoszenia reklamacji wraz z dowodem zakupu w terminie do sześciu miesięcy od dnia zakupu.
  - c. Z przyczyn podanych w punkcie 1. Producent nie gwarantuje bezbłędności Oprogramowania, w szczególności w przypadku niespełnienia przez Oprogramowanie wymogów i oczekiwań użytkownika lub niekompatybilności z wybranymi aplikacjami oraz systemami operacyjnymi. Skutki decyzji zakupu i wyniku zamierzonego oraz niezamierzonego działania Oprogramowania ponosi Użytkownik. Zapis odnosi się również do dołączonej dokumentacji pisemnej. Jeśli Oprogramowanie nie jest zdadne do użytku w myśl punktu 1., Użytkownikowi przysługuje prawo odstąpienia od umowy. Takie samo prawo przysługuje Producentowi, jeżeli wyprodukowanie
-

Oprogramowania użytecznego w myśl punktu 1. nie jest możliwe.

- d. Producent odpowiada tylko za szkody spowodowane umyślnie lub przez rażące zaniedbanie ze strony Producenta. Sprzedawca Oprogramowania nie odpowiada także za szkody spowodowane umyślnie lub przez rażące zaniedbanie sprzedawcy. Maksymalna kwota odszkodowania równa jest kwocie poniesionej przez Użytkownika na zakupienie Oprogramowania.

- 9. Właściwość sądu Sądem właściwym dla wszystkich kwestii spornych wynikających bezpośrednio lub pośrednio z warunków umowy jest sąd odpowiedni dla siedziby Producenta.
- 10. Postanowienia końcowe Unieważnienie tylko niektórych postanowień tej umowy, nie pociąga za sobą unieważnienia pozostałych postanowień. W miejsce unieważnionego postanowienia stosowane jest inne, aktualne postanowienie o najbardziej zbliżonym celu gospodarczym.

Instalując Oprogramowanie Użytkownik akceptuje powyższe warunki licencji. Akceptując warunki licencji wyrażasz zgodę na gromadzenie, przetwarzanie i wykorzystywanie przez G Data Software Sp. z o.o. w Szczecinku Twoich danych, teraz i w przyszłości, zgodnie z polskim prawem, w szczególności Ustawą o ochronie danych osobowych.

Masz prawo wglądu do Twoich danych oraz ich poprawienia lub usunięcia. Podane przez Użytkowników dane osobowe G Data Software Sp. z o.o. w Szczecinku zbiera i przetwarza zgodnie z obowiązującymi przepisami prawa oraz zgodnie z polityką ochrony prywatności G Data Software w poniższym brzmieniu.

Polityka prywatności G Data Software Sp. z o.o.

1. G Data Software Sp. z o.o. w Szczecinku przykłada szczególną wagę do ochrony prywatności Użytkowników. G Data Software Sp. z o.o. w Szczecinku z należytą starannością dobiera i stosuje odpowiednie środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych. W szczególności G Data Software Sp. z o.o. w Szczecinku zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym, jak również przed ich przetwarzaniem z naruszeniem obowiązujących przepisów prawa. G Data Software Sp. z o.o. w Szczecinku sprawuje stałą kontrolę nad procesem przetwarzania danych oraz ogranicza dostęp do danych w możliwie największym stopniu, udzielając stosownych upoważnień tylko wówczas, gdy jest to niezbędne do prawidłowego prowadzenia serwisu.
  2. Podstawą przetwarzania danych osobowych jest zgoda samych Użytkowników, jak również ustawowe upoważnienie do przetwarzania danych niezbędnych w celu realizacji usług świadczonych przez G Data
-

Software Sp. z o.o. w Szczecinku, jak również prowadzenia marketingu bezpośredniego produktów znajdujących się w ofercie G Data Software Sp. z o.o. w Szczecinku.

3. Podanie jakichkolwiek danych osobowych jest dobrowolne. Podanie danych takich jak: imienia i nazwiska, adresu zamieszkania wraz z nazwą kraju i regionu (województwa), adresu e-mail, numeru telefonu kontaktowego, jest konieczne do rejestracji produktu nabytego przez Użytkownika, jak również w celu wykonania zawartej umowy. Użytkownik ma prawo dostępu do treści swoich danych oraz ich poprawiania.
4. Dane podawane przez Użytkownika w trakcie rejestracji są wykorzystywane do celów akcji marketingowych prowadzonych przez G Data Software Sp. z o.o. w Szczecinku, do przesyłania Użytkownikom przez G Data Software Sp. z o.o. w Szczecinku informacji o spółce i świadczonych przez nią usługach, do kontaktowania się z Użytkownikiem w związku ze zbliżającym się terminem wygaśnięcia licencji. Użytkownik może w każdej chwili zrezygnować z otrzymywania tego typu informacji.
5. Dane Użytkowników mogą być udostępniane podmiotom uprawnionym do ich otrzymania na mocy obowiązujących przepisów prawa, w tym właściwym organom wymiaru sprawiedliwości.

6. G Data Software Sp. z o.o. zapewnia Użytkownikom możliwość modyfikacji danych osobowych poprzez zgłoszenie zmiany danych telefonicznie bądź mailowo pracownikowi Działu Obsługi Klienta. W przypadku późniejszej zmiany jakichkolwiek danych, o których mowa w pkt 3. powyżej Użytkownik powinien niezwłocznie je zaktualizować przekazując je za pośrednictwem wyżej wymienionych kanałów.

Copyright © 2011 G Data Software AG Engine A: The Virus Scan Engine and the Spyware Scan Engines are based on BitDefender technologies © 1997-2011 BitDefender SRL. Engine B: © 2011 Alwil Software OutbreakShield: © 2011 Commtouch Software Ltd.

---