

# Rejestr systemu Windows

# Czym jest rejestr systemu Windows?

---

**Rejestr** to centralna hierarchiczna baza danych używana do przechowywania informacji, które są **niezbędne do skonfigurowania systemu**.

W rejestrze zapisane są informacje dotyczące:

- systemu operacyjnego
- sprzętowej konfiguracji
- zainstalowanych aplikacji
- kont użytkowników
- sieci
- powiązań między typami plików a aplikacjami

System Windows zawiera narzędzie do edycji rejestru: **regedit.exe**

# Logiczna budowa rejestru

Logiczna struktura rejestru ma postać hierarchicznego drzewa, która składa się z **kluczy, podkluczy i wartości**.

- **Klucz** to obiekt-kontener przechowujący podklucze i wartości
- **Wartości** to wpis zawierający dane konfiguracyjne określonego typu (każdy klucz ma przynajmniej jedną wartość, tzw. wartość domyślną)
- **Gałąź** to klucz główny wraz z wszystkimi podkluczami i wartościami

The image shows a screenshot of the Windows Registry Editor. On the left, the tree view is expanded to show the path: **Komputer** > **HKEY\_LOCAL\_MACHINE** > **BCD00000000** > **Description**. On the right, a list of registry values is displayed with columns for Name, Type, and Data. Red arrows point from labels to specific elements: 'Gałąź' points to the path, 'Klucz główny' points to 'HKEY\_LOCAL\_MACHINE', 'Podklucz' points to 'Description', 'Nazwa wartości' points to 'KeyName', 'Typ' points to 'REG\_DWORD', and 'Dane' points to '0x00000001 (1)'.

Nazwa	Typ	Dane
(Domyślna)	REG_SZ	(wartość nie ustalona)
GuidCache	REG_BINARY	a3 63 5f a9 b6 a5 d4 01 0e 27
KeyName	REG_SZ	BCD00000000
System	REG_DWORD	0x00000001 (1)
TreatAsSystem	REG_DWORD	0x00000001 (1)

# Fizyczna budowa rejestru

Gałęzie rejestru fizycznie zapisane są w postaci plików (Windows 10):

- C:\Windows\System32\config\SAM
- C:\Windows\System32\config\SECURITY
- C:\Windows\System32\config\SOFTWARE
- C:\Windows\System32\config\SYSTEM
- C:\Windows\System32\config\DEFAULT
- C:\Users\Nazwa użytkownika\NTUSER.DAT

Lokalizacja plików rejestru można sprawdzić w gałęzi:

**HKEY\_LOCAL\_MACHINE\SYSTEM\  
CurrentControlSet\Control\hivelist**

Nazwa	Typ	Dane
(Domyślna)	REG_SZ	(wartość nie ustalona)
\REGISTRY\...	REG_SZ	\Device\HarddiskVolume1\Boot\BCD
\REGISTRY\...	REG_SZ	
\REGISTRY\...	REG_SZ	\Device\HarddiskVolume2\Windows\System32\config\SAM
\REGISTRY\...	REG_SZ	\Device\HarddiskVolume2\Windows\System32\config\SECURITY
\REGISTRY\...	REG_SZ	\Device\HarddiskVolume2\Windows\System32\config\SOFTWARE
\REGISTRY\...	REG_SZ	\Device\HarddiskVolume2\Windows\System32\config\SYSTEM
\REGISTRY\...	REG_SZ	\Device\HarddiskVolume2\Windows\System32\config\DEFAULT
\REGISTRY\...	REG_SZ	\Device\HarddiskVolume2\Windows\ServiceProfiles\LocalService\NTUSER.DAT
\REGISTRY\...	REG_SZ	\Device\HarddiskVolume2\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
\REGISTRY\...	REG_SZ	\Device\HarddiskVolume2\Users\cem\NTUSER.DAT
\REGISTRY\...	REG_SZ	\Device\HarddiskVolume2\Users\cem\AppData\Local\Microsoft\Windows\UsrClass.dat

# Główne klucze rejestru

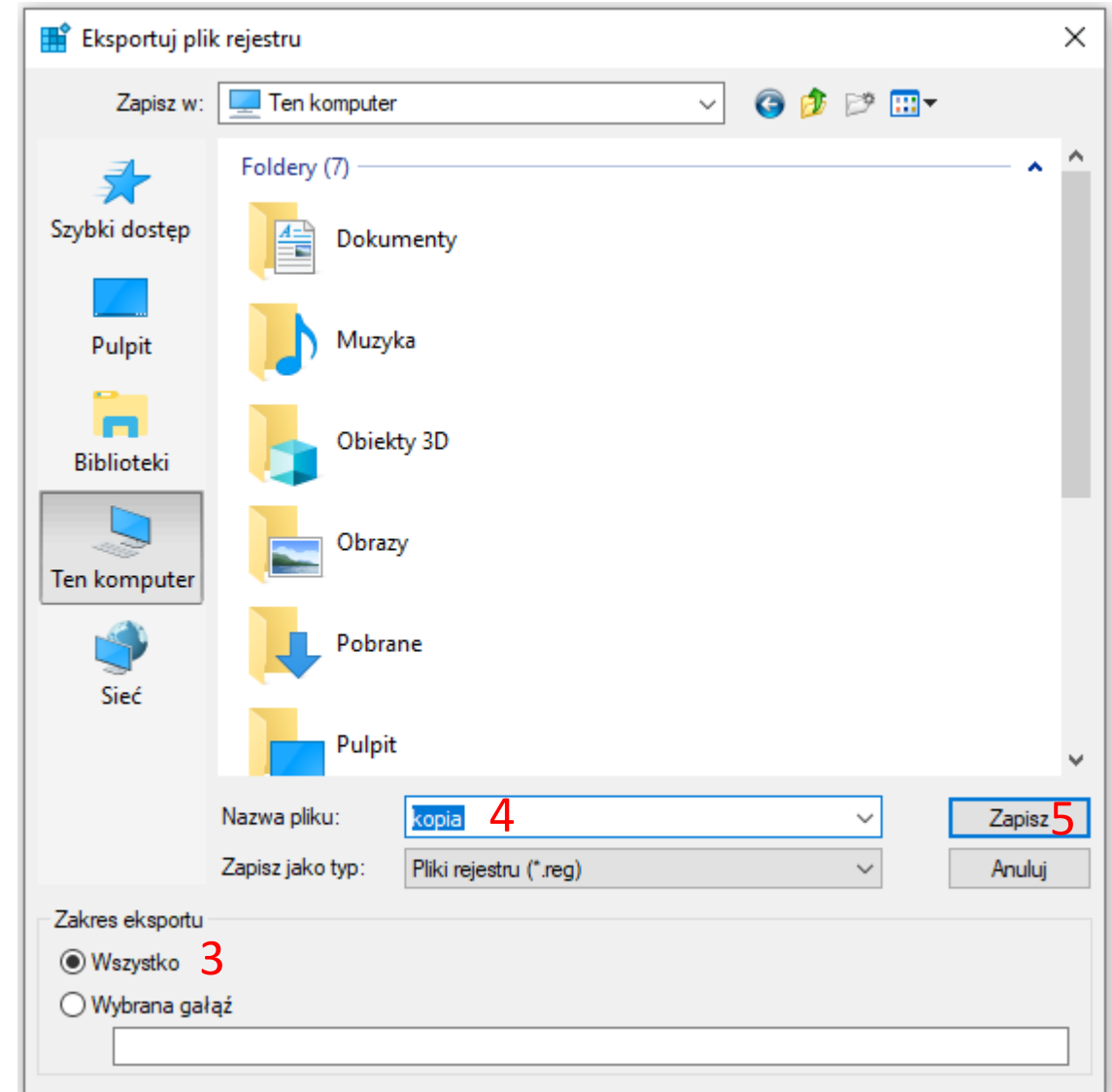
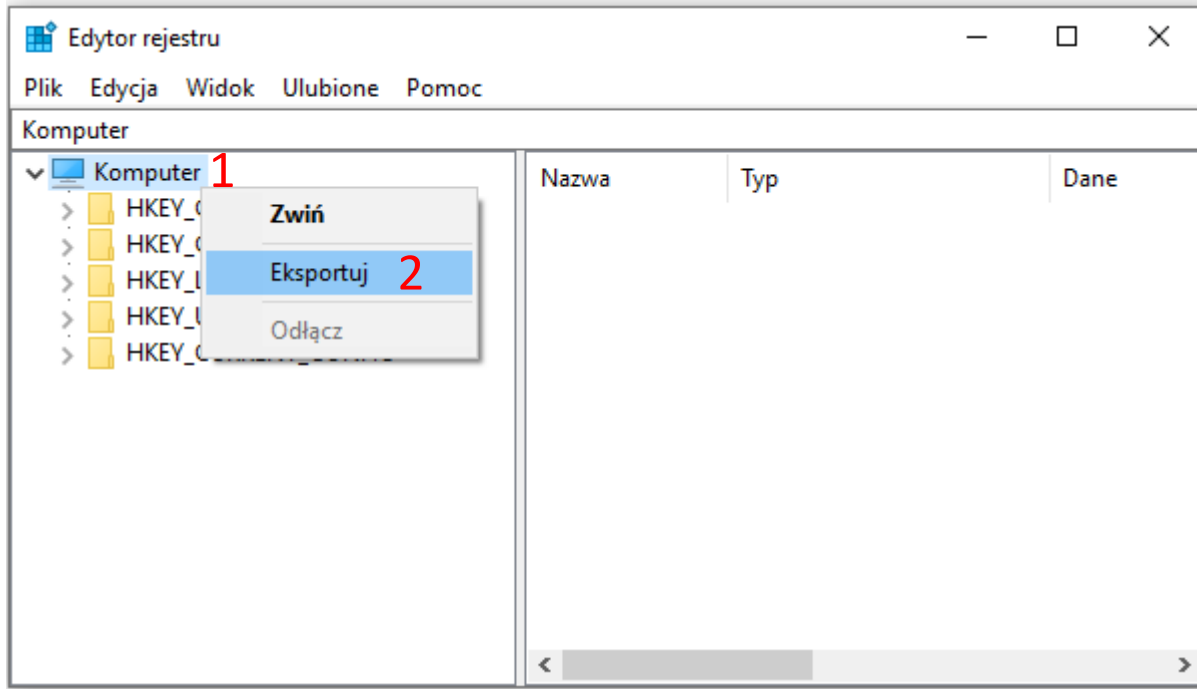
---

Klucz	Zadanie
HKEY_CLASSES_ROOT (HKCR)	Zapisane są tu powiązania typów plików z aplikacjami, które je obsługują
HKEY_CURRENT_USER (HKCU)	Przechowuje ustawienia profilu aktualnie zalogowanego użytkownika.
HKEY_LOCAL_MACHINE (HKLM)	Zawiera najważniejsze informacje o konfiguracji komputera niezbędne do prawidłowego uruchomienia systemu Windows
HKEY_USERS (HKU)	Są to ustawienia profili wszystkich użytkowników, którzy kiedykolwiek logowali się na dany komputer
HKEY_CURRENT_CONFIG (HKCC)	Są to dane konfiguracyjne wykorzystywane przez aktualnie używany profil sprzętowy Windows

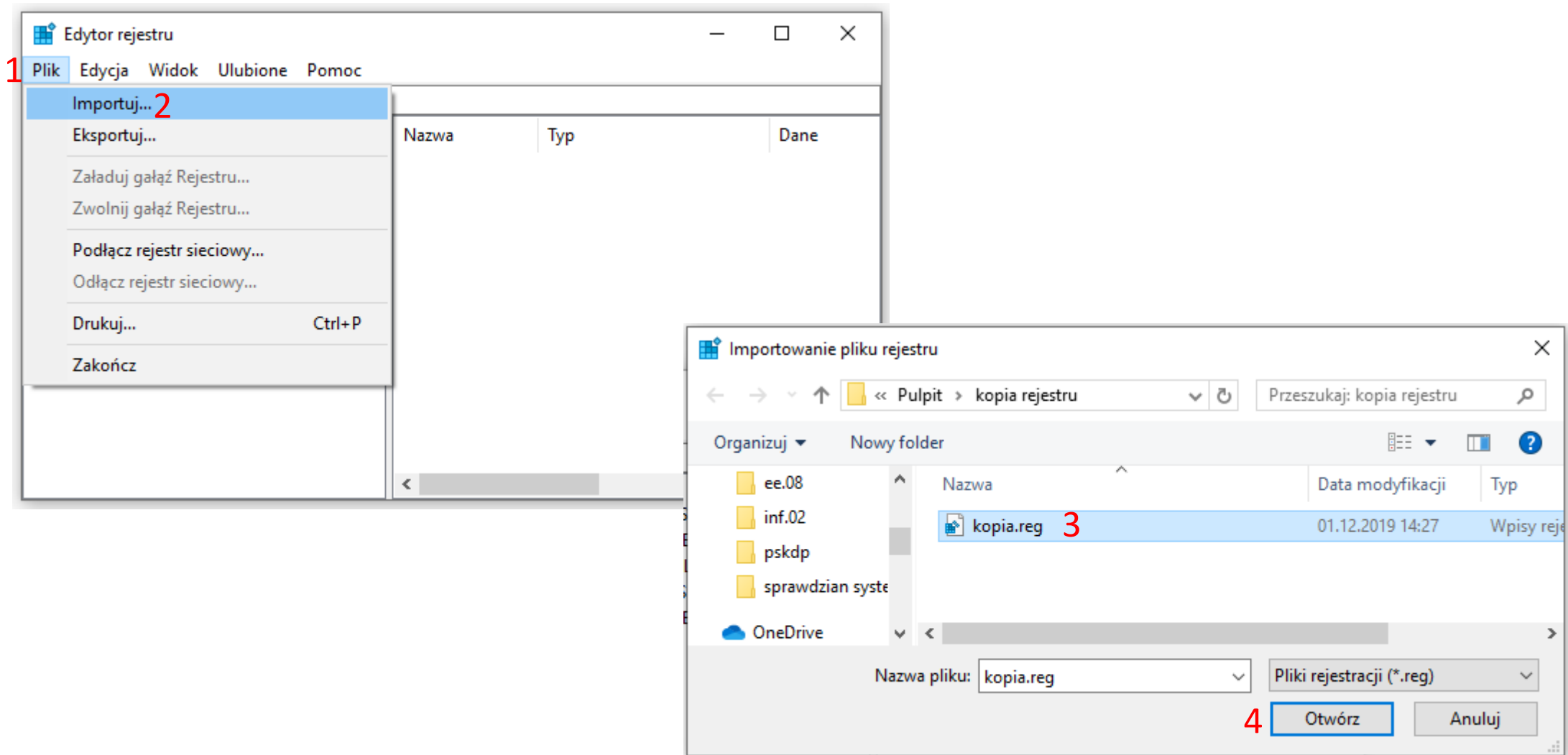
# Typy wartości

Typ (nazwa polska)	Zadanie
<b>REG_SZ</b> (wartość ściągu)	łańcuch tekstowy (napis) zakończony pustym znakiem NULL "\0". Np.: <b>"Tekst\0"</b>
<b>REG_MULTI_SZ</b> (wartość ciągu wielokrotnego)	Wiele połączonych łańcuchów tekstowych. Każdy łańcuch tekstowy musi być zakończony znakiem pustym NULL. Na samym końcu należy dwukrotnie zapisać znak pusty NULL. Np.: <b>"Tekst1\0Tekst2\0Tekst3\0\0"</b>
<b>REG_EXPAND_SZ</b> (wartość ciągu rozwijalnego)	łańcuch tekstowy zakończony znakiem pustym NULL. Może zawierać nazwy zmiennych, które zostaną zastąpiono odpowiednią wartością zmiennej. Np.: <b>"Nazwa użytkownika: %UserName%\0"</b>
<b>REG_BINARY</b> (wartość binarna)	Dane binarne zapisane w notacji szesnastkowej. Np.: <b>A3 63 5F B6</b>
<b>REG_DWORD</b> (wartość DWORD)	32-bitowa liczba całkowita zapisana w notacji szesnastkowej lub dziesiętnej. Np.: <b>0x0000000A</b> (10)
<b>REG_QWORD</b> (wartość QWORD)	64-bitowa liczba całkowita zapisana w notacji szesnastkowej lub dziesiętnej. Np.: <b>0x0000000A</b> (10)

# Program regedit.exe - kopia rejestru

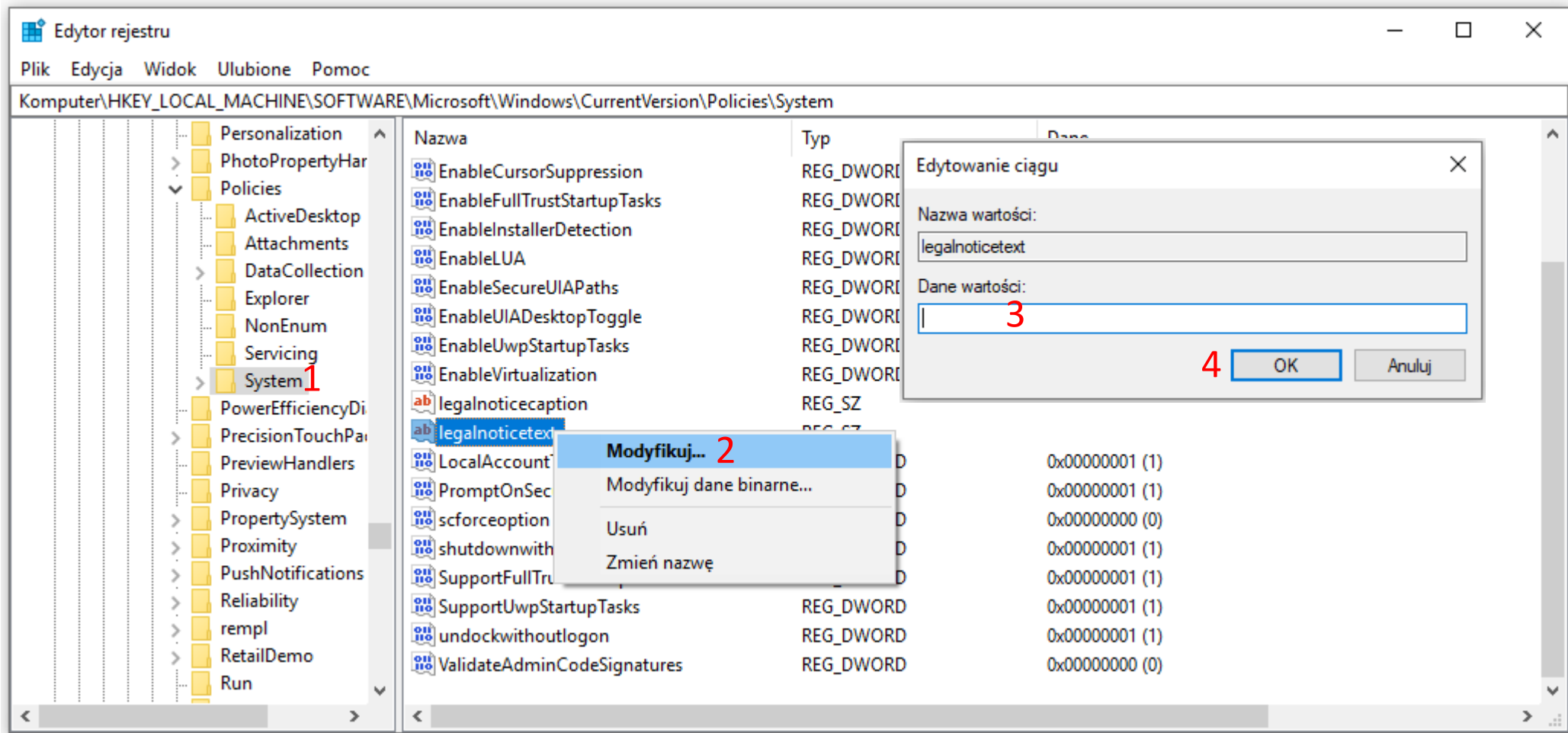


# Program regedit.exe - przywracanie rejestru

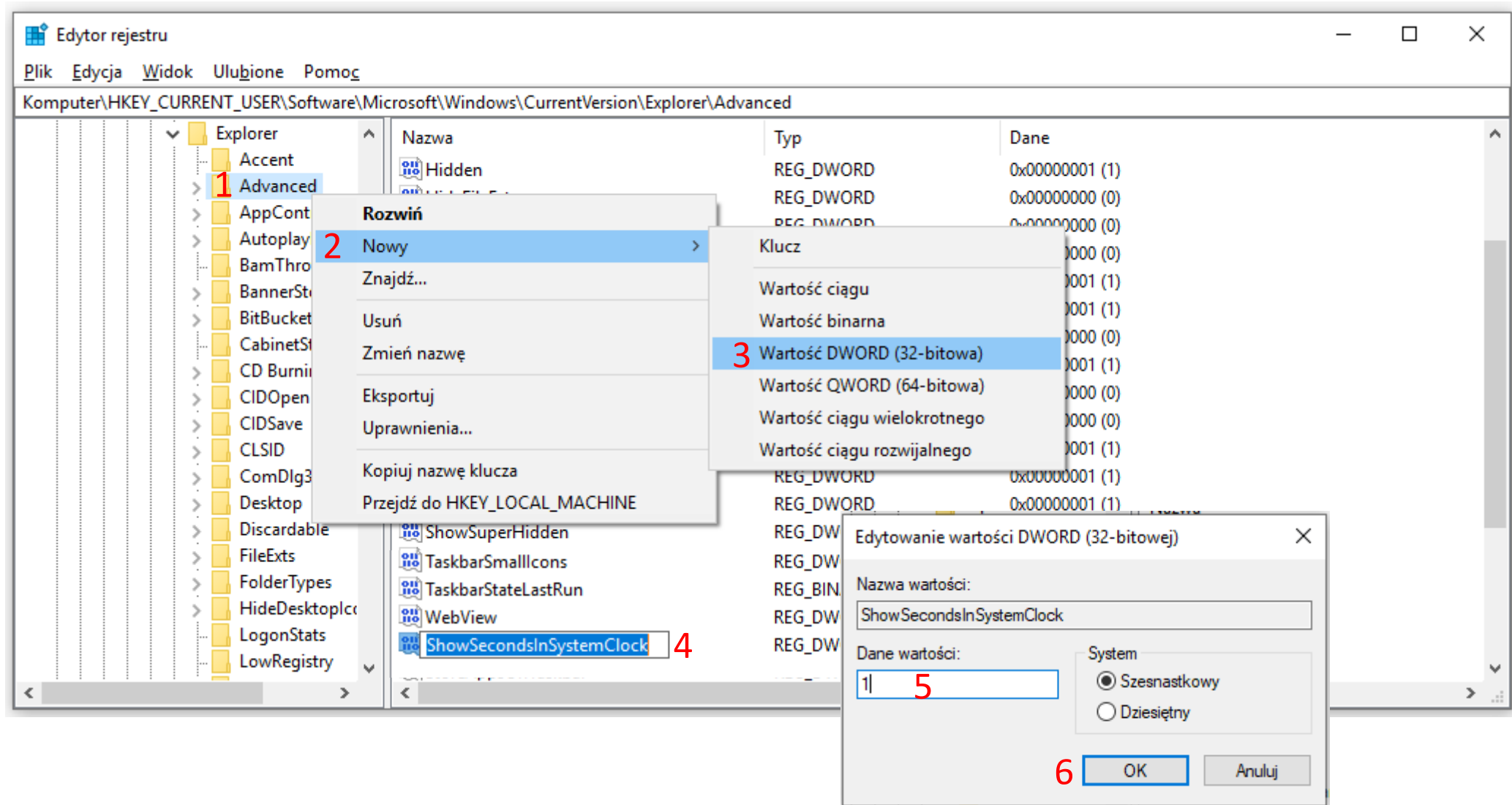




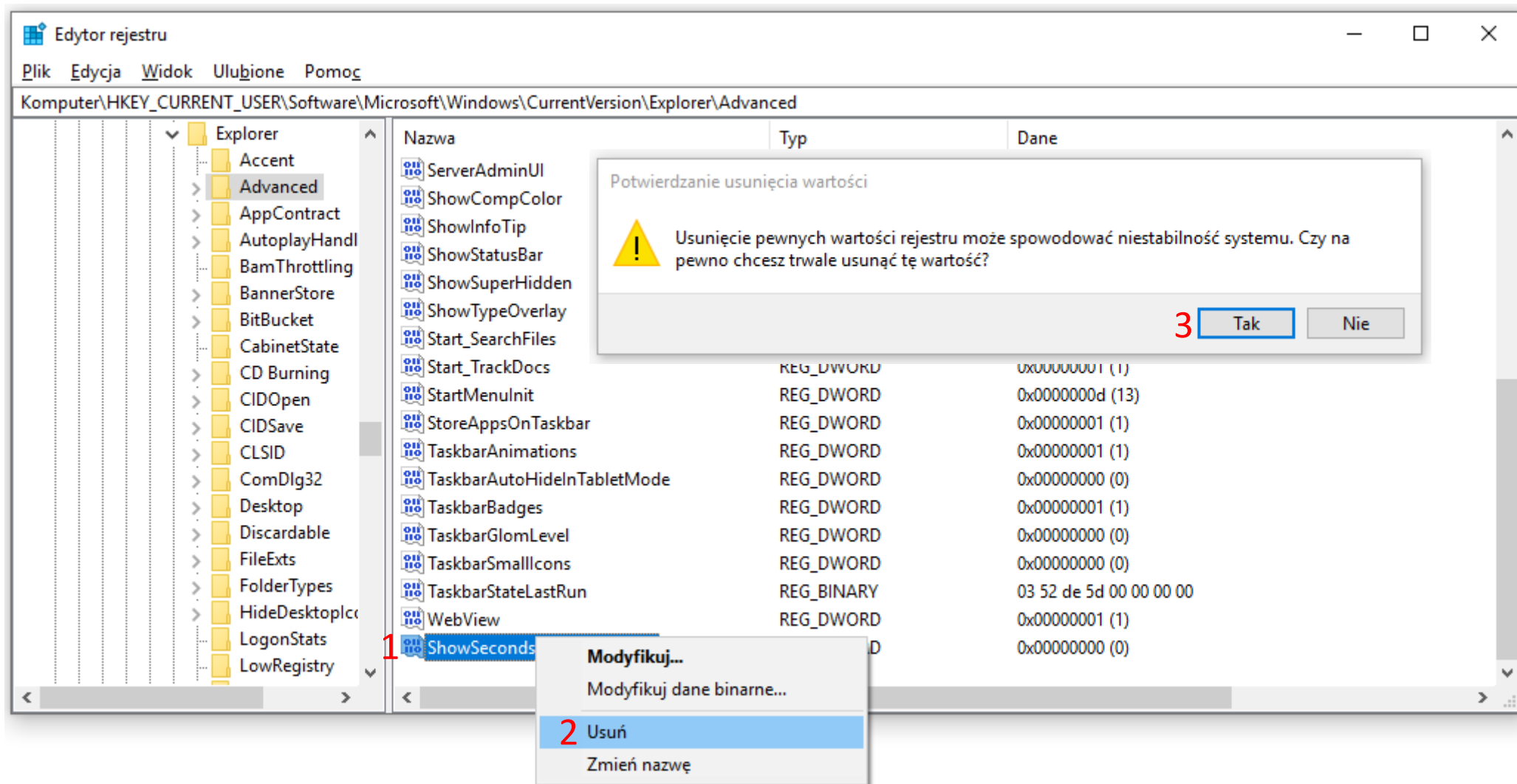
# Program regedit.exe - modyfikacja wartości (REG\_SZ)



# regedit.exe - dodawanie nowej wartości (REG\_DWORD)



# regedit.exe - usuwanie wartości



# Składnia plików .reg

Wersja edytora rejestru

Pusta linia

Ścieżka do danego klucza

Nazwa wartości

Deklaracja typu

właściwości

```
testzdz.reg — Notatnik
Plik Edycja Format Widok Pomoc
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\testzdz]
"Wartość1"="Dane wartości"
"Wartość2"=hex:aa,bb,cc,dd,ee,ff
"Wartość3"=dword:0000000a
"Wartość4"=hex(b):01,00,00,00,00,00,00,00
"Wartość5"=-

[-HKEY_LOCAL_MACHINE\SOFTWARE\testzdz\klucz1]
```

Dane typu REG\_SZ

Dane typu REG\_BINARY

Dane typu REG\_DWORD

Dane typu REG\_QWORD

Znak minus (-) usuwa dany klucz lub wartość

# Scalanie plików .reg

C:\Users\cem\Desktop\kopia rejestru

Zarządzanie

Plik Narzędzia główne Udostępnianie Widok Narzędzia aplikacji

Przeszukaj: ko...

Szybki dostęp

- Pulpit
- Pobrane
- Dokumenty
- Obrazy
- Nowy folder

Elementy: 4 | 1 zaznaczony element. 562 B

desktop.reg desktop1.reg kopia.reg testzdz.reg

Scal 1

Edytuj

Drukuj

Open with Brackets

7-Zip

Edytor rejestru

! Dodanie informacji może spowodować przypadkową zmianę lub usunięcie wartości oraz przerwać poprawne działanie składników. Jeśli nie masz zaufania do źródła informacji zawartych w pliku C:\Users\cem\Desktop\kopia rejestru\testzdz.reg, nie dodawaj go do rejestru.

Czy na pewno chcesz kontynuować?

2 Tak Nie