POLITYKA PRYWATNOŚCI
Mariusz Gomuła
FOUNTAIN OF KNOWLEDGE- NAUKA JĘZYKÓW OBCYCH

obowiązuje od 25.05.2018 r.

W związku ze zmianą przepisów dotyczących ochrony danych osobowych i rozpoczęciem stosowania od dnia 25 maja 2018 roku Rozporządzenia 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 o ochronie danych) "RODO" informujemy, że:

1. **Administratorem danych osobowych Użytkowników Portalu/Serwisu http://www.fountainofknowledge.pl jest Mariusz Gomuła FOUNTAIN OF KNOWLEDGE- NAUKA JĘZYKÓW OBCYCH, dane kontaktowe: Sławno 59, 26-625 Wolanów, NIP: 948-211-41-31, REGON 141946593 e-mail: mario.gomula@gmail.com**

Mariusz Gomuła FOUNTAIN OF KNOWLEDGE- NAUKA JĘZYKÓW OBCYCH
przetwarza dane osobowe w celach:

a. świadczenia usługi, prowadzenia konta Użytkownika w Portalu/Serwisie http://www.fountainofknowledge.pl Podstawą prawną przetwarzania danych jest wykonanie umowy. (art. 6 ust. 1 lit. b RODO),

b. świadczenia usług niewymagających założenia konta takich jak: np. **skontaktowanie się w celu zapytania o świadczonych, wykonanych usługach etc.**

c. marketingowych – podstawą prawną przetwarzania danych jest prawnie uzasadniony interes **Mariusz Gomuła FOUNTAIN OF KNOWLEDGE- NAUKA JĘZYKÓW OBCYCH** – marketing własnych produktów i usług (art. 6 ust. 1 lit. f RODO),

d. rozpatrzenia reklamacji, dochodzenia i obrony w razie zaistnienia wzajemnych roszczeń - podstawą prawną przetwarzania danych jest prawnie uzasadniony interes **Mariusz Gomuła FOUNTAIN OF KNOWLEDGE- NAUKA JĘZYKÓW OBCYCH** (art. 6 ust. 1 lit. f RODO),

e. wysyłki informacji handlowych drogą elektroniczną - wyłącznie w przypadku wyrażenia zgody przez Użytkownika. Podstawą prawną przetwarzania danych jest zgoda (art. 6 ust. 1 lit. b RODO),

2. Podanie danych osobowych jest dobrowolne, lecz niezbędne w celu korzystania z Portalu http://www.fountainofknowledge.pl oraz jest niezbędne do realizowania umowy o świadczenie usług, w przypadku niepotwierdzenia danych niemożliwe jest kontynuowanie umowy.

3. Dane osobowe przetwarzane będą przez okres niezbędny dla wykonania usługi, a po tym okresie dla celów i przez czas oraz w zakresie wymaganym przez przepisy prawa lub dla zabezpieczenia ewentualnych roszczeń, lub do czasu cofnięcia udzielonej zgody.

4. **Odbiorcami danych osobowych będą:**

. http://www.fountainofknowledge.pl a także podmioty świadczące usługi związane z bieżącą działalnością **Mariusz Gomuła FOUNTAIN OF KNOWLEDGE- NAUKA JĘZYKÓW OBCYCH** na podstawie zawartych umów powierzenia przetwarzania danych osobowych zgodnie z art. 28 RODO,

a. uprawnione organy państwowe na podstawie pisemnego wniosku.

5. Każdej osobie, w zakresie wynikającym z przepisów prawa, przysługuje prawo do dostępu do swoich danych oraz ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo wniesienia sprzeciwu wobec przetwarzania, prawo do przenoszenia danych, a także prawo cofnięcia udzielonej zgody w dowolnym momencie. Cofnięcie zgody nie ma wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.

6. W przypadku wątpliwości związanych z przetwarzaniem danych osobowych każda osoba może zwrócić się do **Mariusz Gomuła FOUNTAIN OF KNOWLEDGE- NAUKA JĘZYKÓW OBCYCH** z prośbą o udzielenie informacji.

7. Niezależnie od powyższego każdemu przysługuje prawo wniesienia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych.

Ponadto, informujemy, że:

1. Usługodawca rejestruje adresy IP Usługobiorców, jak również informacje o rozpoczęciu, zakończeniu oraz zakresie korzystania z Usług, które to informacje zapisywane są w logach systemowych.

2. Serwis/Portal **Mariusz Gomuła FOUNTAIN OF KNOWLEDGE- NAUKA JĘZYKÓW OBCYCH** używa "cookies" w celu personalizacji Usług i treści Portalu.

ZAŁĄCZNIK

ZAGROŻENIA ZWIĄZANE Z KORZYSTANIEM Z USŁUG ORAZ ŚRODKI TECHNICZE DOSTĘPNE USŁUGOBIORCOM W CELU ICH ZMINIMALIZOWANIA

Wirus komputerowy – program komputerowy, który w sposób celowy powiela się bez zgody użytkownika. Wirus komputerowy do swojej działalności wymaga nosiciela w postaci programu komputerowego, poczty elektronicznej itp. Wirusy wykorzystują słabość zabezpieczeń systemów komputerowych lub właściwości systemów oraz niedoświadczenie i beztroskę użytkowników.

Złośliwe oprogramowanie, malware (z ang. malicious software) - aplikacje, skrypty i ingerencje mające szkodliwe, przestępcze lub złośliwe działanie w stosunku do użytkownika komputera.

Robaki – wirusy rozmnażające się tylko przez sieć. Nie potrzebują programu "żywiciela" tak jak typowe wirusy. Często powielają się pocztą elektroniczną.

Trojan – Ukrywa się pod nazwą lub w części pliku, który użytkownikowi wydaje się pomocny. Oprócz właściwego działania pliku zgodnego z jego nazwą, trojan wykonuje operacje w tle szkodliwe dla użytkownika np. otwiera port komputera, przez który może być dokonany atak hakera.

Backdoor – przejmuje kontrolę nad zainfekowanym komputerem umożliwiając wykonanie na nim czynności administracyjnych łącznie z usuwaniem i zapisem danych. Podszywa się pod pliki i programy, z których często korzysta użytkownik. Umożliwia intruzom administrowanie systemem operacyjnym poprzez Internet. Wykonuje zadania wbrew wiedzy i woli ofiary.

Spyware – oprogramowanie zbierające informacje o osobie fizycznej lub prawnej bez jej zgody. Występuje często jako dodatkowe i ukryte komponenty większego programu, odporne na usuwanie i ingerencję użytkownika. Spyware zmienia wpisy do rejestru systemu operacyjnego i ustawienia użytkownika. Potrafi pobierać i uruchamiać pliki pobrane z sieci.

Exploit – kod umożliwiający zdalne przejęcie kontroli nad komputerem poprzez sieć, wykorzystując do tego celu dziury w programach i systemach operacyjnych.

Root kit – jedno z najniebezpieczniejszych narzędzi hakerskich. Podstawowym zadaniem rootkita jest ukrywanie procesów określonych przez hakera, a zmierzających do przejęcia kontroli nad komputerem użytkownika.

Keylogger – Odczytuje i zapisuje wszystkie naciśnięcia klawiszy użytkownika. Dzięki temu adresy, kody, cenne informacje mogą dostać się w niepowołane ręce.

Dialery – programy łączące się z siecią przez inny numer dostępowy niż wybrany przez użytkownika. Dialery szkodzą tylko posiadaczom modemów telefonicznych analogowych i cyfrowych ISDN.

SQL/URL injection – forma ataku na bazę danych poprzez stronę WWW i komendy języka SQL. Służy wyciąganiu informacji z bazy danych niedostępnych dla zwykłego użytkownika. Atakujący może zmodyfikować zapytanie kierowane do bazy danych poprzez modyfikację adresu URL o nieautoryzowane polecenia języka SQL.

Obrona przed szkodliwym oprogramowaniem:

- instalacja oprogramowania antywirusowego, włączona zapora sieciowa (firewall)

- aktualizacja oprogramowania
- nie otwieranie załączników poczty elektronicznej niewiadomego pochodzenia
- czytanie okien instalacyjnych aplikacji
- wyłączenie makr w MS Excel i Word
- regularne całościowe skany systemu programem antywirusowym
- przy płatnościach drogą elektroniczną upewnienie się że transmisja danych będzie szyfrowana