POLITYKA BEZPIECZEŃSTWA

Data i miejsce sporządzenia dokumentu:	05/01/2017
Ilość stron:	5

1. WSTĘP

1.1. INFORMACJE OGÓLNE

1. Administratorem danych jest administrator serwera odpowiadającego za komunikację.
2. Dane osobowe są zbierane w celu identyfikacji użytkownika użytkującego aplikację “ChatApp”.
3. Niniejszy dokument jest zgodny z:
    a. Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j.Dz.U.z2002r., Nr 101, poz.926 z późn.zm.),
    b. Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych,
    c. Ustawą o ochronie informacji niejawnych z dnia 22 stycznia 1999 r. (Dz. U. NR 11, poz.95 z późn.zm.),
    d. Rozporządzeniem Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. Nr 171 poz.1433)

1.2. ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ BEZPIECZEŃSTWA ORAZ ZAKRES ZASTOSOWANIA

1. Dane osobowe jak i niejawne są przechowywane bazie danych stworzonej w systemie PostgreSQL.
2. Dane osobowe:
    a. Mail
    b. Nazwa użytkownika Google+
    c. Zdjęcie z konta Google+
3. Dane niejawne
    a. Wiadomości wysyłane jak i otrzymywane przez użytkowników aplikacji
4. Dane osobowe są uzyskiwane dzięki systemowi Google+ Api wydanego przez firmę Google LLC

5. Integralność, poufność i rozliczalność danych gwarantuje system Google+ Api wydany przez firmę Google LLC

1.3. WYJAŚNIENIE TERMINÓW UŻYWANYCH W DOKUMENCIE POLITYKI BEZPIECZEŃSTWA

1. **Administrator danych** – organ, jednostka organizacyjna, podmiot lub osoba, o których mowa w art. 3 Ustawy o ochronie danych osobowych, decydująca o celach i środkach przetwarzania danych osobowych,
2. **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
3. **przetwarzanie danych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
4. **poufność danych** – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.

2. OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

2.1. INFORMACJE OGÓLNE

1. Pewien katalog osób zajmujących określone stanowisko (pełniących określone funkcje) i zarazem odpowiadających za powyższe czynności jest niezmienny:
    a. Administrator Danych,
    b. Osoby wykonujące pracę bądź świadczące usługi cywilnoprawne na rzecz Administratora Danych Osobowych, które uzyskały upoważnienie do przetwarzania danych osobowych.

2.2. OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Każda osoba, która uzyskała upoważnienie do przetwarzania danych osobowych zobowiązana jest do ich ochrony w sposób zgodny z przepisami Ustawy, Rozporządzenia, Polityki Bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym.
2. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia.

3. Upoważnienie do przetwarzania danych osobowych

1. Za przetwarzanie danych osobowych odpowiedzialny jest Administrator Danych Osobowych.

2. Upoważnienie do pełnienia tej funkcji jak i wszelkie uprawniania otrzymuje od prezesa spółki Inba z.o.o. Na podstawie dokumentu nr. 2137 z regulaminu spółki

4. UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

1. Ustawa o ochronie danych osobowych przewiduje możliwość powierzenie przetwarzania danych osobowych przez Administratora Danych zewnętrznym podmiotom. Może się to odbywać wyłącznie na drodze umowy powierzenia, w której należy określić zbiór, który zostanie przekazany, cel tego przekazania oraz zakres planowanego przetwarzania danych przez inny podmiot.

5. Ogólne zasady bezpieczeństwa obowiązujące przy przetwarzaniu danych osobowych

1. Za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze, indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik mający dostęp do danych.
2. Pracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.

6. Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych

1. Każda osoba, która poweźmie wiadomość w zakresie naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe bądź posiada informacje mogące mieć wpływ na bezpieczeństwo danych osobowych, jest zobowiązana fakt ten niezwłocznie zgłosić Administratorowi Danych Osobowych.
2. Po potwierdzeniu powiadomienia Administrator Danych Osobowych powinien:
    a. niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków, a następnie ustalić przyczyny, lub sprawców zaistniałego zdarzenia, jeżeli jest to możliwe,
    b. zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,
    c. udokumentować wstępnie zaistniałe naruszenie,
3. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu, Administrator Danych Osobowych, zasięga niezbędnych opinii i proponuje postępowanie naprawcze (w tym ustosunkowuje się do kwestii ewentualnego

odtworzenia danych z zabezpieczeń) i zarządza termin wznowienia przetwarzania danych.

7. Kontrola przetwarzania i stanu zabezpieczenia danych osobowych

1. Nadzór i kontrolę nad ochroną danych osobowych przetwarzanych w ChatApp sprawuje Administrator Danych Osobowych.
2. Administrator Danych Osobowych Informacji dokonuje czynności kontrolnych w ramach sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, zgodnie z art. 36 ust. 2 pkt 1 ppkt a) Ustawy o ochronie danych osobowych.
3. Sprawdzenia dokonywane jest przez Administratora Danych Osobowych dla Administratora Danych, bądź dla Generalnego Inspektora Ochrony Danych Osobowych, gdy ten na podstawie przysługujących mu kompetencji zwróci się o to do Administrator Danych Osobowych.
4. Administrator Danych Osobowych przeprowadza sprawdzenie w trybie:
    a. sprawdzenia planowego - według opracowanego planu sprawdzeń;
    b. sprawdzenia doraźnego - w przypadku nieprzewidzianym w planie sprawdzeń, w sytuacji powzięcia wiadomości o naruszeniu ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takiego naruszenia, niezwłocznie po powzięciu przez Administratora Danych Osobowych takich informacji;
    c. sprawdzenia w przypadku zwrócenia się o to przez Generalnego Inspektora Ochrony Danych Osobowych.
5. Administrator Danych Osobowych opracowuje plan sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
6. W toku sprawdzenia Administrator Danych Osobowych dokonuje i dokumentuje czynności, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz do opracowania sprawozdania.
7. Po zakończeniu sprawdzenia Administrator Danych Osobowych przygotowuje sprawozdanie w tym zakresie. Sprawozdanie sporządzane jest w postaci elektronicznej albo w postaci papierowej.
8. Administrator Danych Osobowych ma prawo do kontroli podmiotów, którym powierzono przetwarzanie danych osobowych w trybie określonym w Polityce Bezpieczeństwa, o ile w umowie o powierzeniu przetwarzania danych osobowych istnieją stosowne zapisy w tym zakresie.

11. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

1. W celu zapewnienia odpowiedniego bezpieczeństwa podczas logowania został użyty system OAuth2.

2. Bezpieczeństwo danych wymaganych do zalogowania stoi po stronie systemu Google+ Api, wydanego przez firmę Google LLC.
3. Bezpieczeństwo wysyłanych wiadomości jest gwarantowane przez protokół SSL oraz platformę Phoenix.
4. Bezpieczeństwo serwera stoi po stronie firmy XYZ, która świadczy usługi udostępniania serwera
5. Bezpieczeństwo bazy danych gwarantuje system PostgresSQL.