Umowa powierzenia przetwarzania danych osobowych

Niniejsza Umowa powierzenia przetwarzania danych osobowych Calamari („Umowa powierzenia”) zawiera postanowienia dotyczące warunków przetwarzania danych osobowych zgodnie z Regulaminem Calamari („Regulamin”). Niniejsza Umowa stanowi aneks do Regulaminu i wchodzi w życie po jej włączeniu do Regulaminu. Po włączeniu do Regulaminu Umowa powierzenia będzie stanowić jego część.

Akceptując niniejszą Umowę powierzenia w imieniu Klienta, oświadczają Państwo, że:

(a) mają pełną zdolność prawną do zaciągania zobowiązań wynikających z niniejszej Umowy powierzenia w imieniu Klienta,
(b) przeczytali i rozumieją Państwo niniejszą Umowę,
(c) zgadzają się Państwo w imieniu Klienta na postanowienia niniejszej Umowy,
(d) ponadto informacje udzielone podczas rejestracji są poprawne, dokładne i zgodne z Państwa najlepszą wiedzą.

Strony oświadczają i uzgadniają, że w odniesieniu do jakichkolwiek danych osobowych na Koncie firmowym Klienta:

(a) Klient będzie Administratorem danych osobowych, zaś
(b) Calamari będzie Podmiotem przetwarzającym te dane.

Każda ze stron będzie przestrzegać zobowiązań, które będą ich dotyczyć na mocy Przepisów o ochronie danych osobowych w odniesieniu do przetwarzania danych osobowych.

Niniejsza Umowa powierzenia obejmuje:

1. Specyfikację przetwarzania danych osobowych,
2. Techniczne i organizacyjne środki bezpieczeństwa,
3. Listę podmiotów, którym podzlecono przetwarzanie danych osobowych.

Specyfikacja przetwarzania danych osobowych

Definicje

„**Konto**” („Konto firmowe Klienta” lub „Konto firmowe”) oznacza łącznie informacje, dane płatnicze i uwierzytelniające, Dane osobowe dodane i używane przez Klienta w ramach Usług Calamari;

„**Regulamin**” oznacza regulamin obowiązujący Klienta i Calamari;

„**Calamari**” („Sprzedawca”) oznacza następujący podmiot: Calamari spółka z ograniczoną odpowiedzialnością spółka komandytowa z siedzibą w Warszawie, ul. Chmielna 2/31, 00-020 Warszawa, wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego, prowadzonego przez Sąd Rejonowy dla m.st. Warszawy w Warszawie pod numerem KRS 0000720781, NIP 5252741247, REGON 369568795, który zajmuje się rozwojem, zarządzaniem i świadczeniem Usług Calamari;

„**Klient**” („Państwo”) oznacza jakąkolwiek organizację, która postanowi wdrożyć u siebie Calamari;

„**Administrator**” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;

„**Przepisy o ochronie danych osobowych**” oznaczają Ogólne rozporządzenie UE o ochronie danych 2016/679 oraz polską “Ustawę o ochronie danych osobowych, z dnia 10 maja 2018 r.” (Dz.U. 2018 poz. 1000);

„**Inspektor ochrony danych**” jest zdefiniowany w Ogólnym rozporządzeniu UE o ochronie danych 2016/679, art. 37–39;

„**Osoba, której dane dotyczą**” oznacza osobę, której dotyczą Dane osobowe;

„**Ogólne rozporządzenie UE o ochronie danych**” oznacza Rozporządzenie 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;

„**Dane osobowe**” oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

„**Naruszenie ochrony danych osobowych**” oznacza naruszenie bezpieczeństwa Calamari prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do Danych osobowych w systemach zarządzanych przez Calamari; Naruszenie ochrony danych osobowych nie obejmuje nieudanych prób lub działań, które nie zagrażały bezpieczeństwu Danych osobowych, w tym nieudanej próby zalogowania się, wywoływania poleceń ping, skanowania portu, ataków DoS ani innych ataków sieci na zaporę ogniową (firewall) lub systemy sieciowe;

„**Podmiot przetwarzający**” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza Dane osobowe w imieniu Administratora;

„**Wrażliwe dane osobowe**” oznaczają wszelkie dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby oraz dane dotyczące popełnienia lub podejrzenia popełnienia jakiegokolwiek czynu zabronionego;

„**Podmiot, któremu podzlecono przetwarzanie danych osobowych**” oznacza osoby trzecie upoważnione na mocy niniejszej Umowy powierzenia przetwarzania danych osobowych do posiadania logicznego dostępu do Danych osobowych i przetwarzania ich w celu świadczenia części Usług Calamari i jakiegokolwiek wsparcia technicznego;

„**Usługa(-i)**” oznacza usługi online wspierajace zarządzanie personelem, których rozwojem, funkcjonowaniem i utrzymaniem zajmuje się Calamari, lub pomocnicze produkty i usługi offline lub online świadczone na rzecz Klienta przez Calamari, do których Klient otrzymuje dostęp;

„**Użytkownik(-cy)**” oznacza pracowników, przedstawicieli, konsultantów, podwykonawców lub pełnomocników Klienta, których upoważniono do korzystania z Usług i którzy otrzymali od Klienta (lub Calamari na życzenie Klienta) identyfikatory i hasła użytkownika;

Jakiekolwiek sformułowanie znajdujące się po wyrażeniu „w tym”, „włączając” lub podobnym wyrażeniu będzie interpretowane jako przykładowe i nie będzie ograniczać znaczenia słów poprzedzających to wyrażenie. Wszelkie przykłady przytoczone w niniejszej Umowie powierzenia mają charakter obrazujący i nie są jedynymi przykładami danego konceptu.

Zastosowanie niniejszej Umowy powierzenia

Niniejsza Umowa powierzenia ma zastosowanie:

(a) w przypadku, gdy Klient potwierdził kliknięciem akceptację niniejszej Umowy lub
(b) w przypadku, gdy niniejszą Umowę włączono do Regulaminu poprzez odniesienie.

Data wejścia w życie niniejszej Umowy powierzenia to odpowiednio:

(a) 25 maja 2018 r., w przypadku gdy Klient potwierdził kliknięciem akceptację lub strony w inny sposób zaakceptowały postanowienia niniejszej Umowy w tym dniu lub wcześniej, lub
(b) data, w której Klient potwierdził kliknięciem akceptację lub strony w inny sposób zaakceptowały postanowienia niniejszej Umowy, jeżeli data ta przypadnie po 25 maja 2018 r., lub
(c) data, w której Klient potwierdził kliknięciem akceptację lub strony w inny sposób zaakceptowały postanowienia Regulaminu Calamari, do którego niniejszą Umowę włączono poprzez odniesienie, jeżeli data ta przypadnie po 25 maja 2018 r.

Szczegółowe informacje dotyczące przetwarzania

(a) Kategorie Osób, których dane dotyczą. Pracownicy, przedstawiciele, konsultanci, podwykonawcy lub pełnomocnicy Administratora. Wszystkie osoby, których Dane osobowe są przechowywanie w ramach Usług Calamari przez Administratora (lub przez Calamari na życzenie Administratora).

(b) Rodzaje Danych osobowych. Podmiot przetwarzający może przetwarzać następujące dane:
   (i) wszystkie dane (w tym wszelkie potencjalnie Wrażliwe dane osobowe), które są przechowywanie w ramach Usług Calamari przez Administratora, Użytkowników lub Podmiot przetwarzający na życzenie Administratora, w tym:
      (1) dane kontaktowe, daty urodzenia, adres zamieszkania, imię pracownika, nazwisko pracownika, adresy e-mail, numery telefonu, płeć, szczegóły dotyczące wysokości wynagrodzenia i świadczenia emerytalnego, bezpośredniego przełożonego, datę zatrudnienia, datę rozwiązania stosunku pracy, stan cywilny, liczbę dzieci, prywatny adres e-mail, imię i nazwisko osoby do kontaktu w sytuacjach nagłych, numer telefonu osoby do kontaktu w sytuacjach nagłych, zapis zwolnień chorobowych, niektóre dane medyczne, grafik pracy, dział, świadczenie urlopowe, daty i godziny nieobecności w pracy, przyczyny nieobecności w pracy,
   (ii) korespondencję między Podmiotem przetwarzającym a Administratorem i Użytkownikami ze strony Administratora,
   (iii) dane nawigacyjne (w tym informacje o użyciu strony, lokalizacji i ruchu, logi strony, zasoby, z których Państwo korzystają, adres IP, identyfikator online i pozostałe dane dotyczące komunikacji).

Administrator oświadcza i zapewnia, że:
(a) ma prawo do przekazywania Danych osobowych (w tym Wrażliwych danych osobowych, jeżeli ma to zastosowanie) Podmiotowi przetwarzającemu w celu otrzymania Usługi oraz
(b) jest wyłącznie odpowiedzialny za uzyskiwanie wszelkich wymaganych zgód, upoważnień i pozwoleń od Użytkowników i osób trzecich oraz przekazywanie

Użytkownikom i osobom trzecim wszelkich wymaganych powiadomień (tam, gdzie ma to zastosowanie), aby mogli Państwo przekazać te informacje Podmiotowi przetwarzającemu.

(c) Przedmiot i charakter przetwarzania. Przedmiotem przetwarzania Danych osobowych przez Podmiot przetwarzający jest świadczenie Usług na rzecz Administratora, które obejmuje przetwarzanie Danych osobowych.

(d) Cel przetwarzania. Dane osobowe będą przetwarzane w celu świadczenia usług wymienionych i ustalonych w Regulaminie, w tym w celu:
  (i) administrowania i zarządzania kontem Administratora,
  (ii) udzielenia Administratorowi wsparcia dla użytkownika końcowego.
  (iii) moderowania i wstępnej konfiguracji Konta,
  (iv) badań i analizy w celu doskonalenia jakości Usługi,
  (v) zapewnienia bezpieczeństwa Administratorowi i innym użytkownikom Usługi,
  (vi) wysyłania do Administratora dalszych informacji na temat Usług na żądanie Administratora,
  (vii) wysyłania Administratorowi powiadomień o wszelkich zmianach w Usłudze.

(e) Czas trwania przetwarzania. Dane osobowe będą przetwarzane przez okres obowiązywania umowy o świadczenie usług zgodnie Regulaminem i przez okres od wygaśnięcia umowy o świadczenie usług do usunięcia Danych osobowych Administratora przez Podmiot przetwarzający zgodnie z niniejszą Umową powierzenia.

Odpowiedzialność Administratora

Administrator jest wyłącznie odpowiedzialny za zgodność z wymogami ustawowymi w zakresie ochrony danych i prywatności, w szczególności w zakresie ujawniania i przekazywania Danych osobowych Podmiotowi przetwarzającemu i przetwarzania Danych osobowych.

Niniejsza Umowa powierzenia stanowi pełne i ostateczne wytyczne Administratora dla Podmiotu przetwarzającego w zakresie Danych osobowych, zaś wszelkie dodatkowe wytyczne wychodzące poza zakres Umowy wymagają uprzedniej pisemnej zgody stron.

Odpowiedzialność Podmiotu przetwarzającego

Przestrzeganie wytycznych. Strony oświadczają i uzgadniają, że Klient jest Administratorem Danych osobowych, zaś Calamari jest Podmiotem przetwarzającym te Dane. Podmiot przetwarzający będzie gromadził, przetwarzał i używał Danych osobowych wyłącznie zgodnie z zakresem wytycznych Administratora. Jeżeli Podmiot przetwarzający uzna, że wytyczne Administratora naruszają Przepisy o ochronie danych osobowych, niezwłocznie poinformuje o tym Administratora.

Inspektor ochrony danych. Podmiot przetwarzający wyznacza Inspektora ochrony danych, który wykonuje swoje obowiązki zgodnie z art. 38 i 39 Ogólnego rozporządzenia UE o ochronie danych. Administrator może skontaktować się z Inspektorem ochrony danych w dowolnym momencie drogą elektroniczną: dpo@calamari.io.

Bezpieczeństwo. Podmiot przetwarzający podejmie odpowiednie techniczne i organizacyjne środki bezpieczeństwa, aby odpowiednio chronić Dane osobowe przed przypadkowym lub niezgodnym z prawem zniszczeniem, utraceniem, zmodyfikowaniem, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem. Środki te obejmują między innymi te, które opisano w sekcji „Techniczne i organizacyjne środki bezpieczeństwa". Podmiot przetwarzający wdroży środki mające na celu bezpieczeństwo danych, aby zapewnić poziom bezpieczeństwa odpowiedni do ryzyka dotyczącego poufności, integralności, dostępności i stabilności systemów w znaczeniu art. 32 par. 1 Ogólnego rozporządzenia UE o ochronie danych.

Poufność. Podmiot przetwarzający dopilnuje, aby personel upoważniony przez Podmiot przetwarzający do przetwarzania Danych osobowych w jego imieniu podlegał zobowiązaniu do zachowania poufności w odniesieniu do Danych osobowych. Zobowiązanie do zachowania poufności będzie obowiązywać po zakończeniu wyżej wymienionych czynności.

Przypadki Naruszenia ochrony danych osobowych. Podmiot przetwarzający powiadomi Administratora niezwłocznie (ale nie później niż po upływie 72 godzin) po stwierdzeniu Naruszenia ochrony danych osobowych dotyczącego Danych osobowych.

Na żądanie Administratora Podmiot przetwarzający niezwłocznie przekaże Administratorowi wszelkie zasadne wsparcie, aby umożliwić Administratorowi zgłoszenie przypadków naruszenia ochrony danych osobowych właściwym organom lub poszkodowanym Osobom, których dane dotyczą, jeżeli Administrator jest do tego zobowiązany na mocy Przepisów o ochronie danych osobowych.

Powiadomienia dotyczące przypadków Naruszenia ochrony danych osobowych mogą obejmować:

(a) charakter Naruszenia ochrony danych osobowych,
(b) datę i godzinę wystąpienia i wykrycia Naruszenia ochrony danych osobowych,
(c) liczbę Osób, których dane dotyczą, dotkniętych incydentem,
(d) kategorie odnośnych Danych osobowych,
(e) nazwę i dane kontaktowe osoby odpowiedzialnej za kontakty ze strony Inspektora ochrony danych.

Żądania osoby, której dane dotyczą. Podmiot przetwarzający udzieli zasadnej pomocy, aby Administrator mógł odpowiedzieć na każde żądanie ze strony Osoby, której dane dotyczą, zwracającej się o wykonanie swojego prawa na mocy Przepisów o ochronie danych osobowych w odniesieniu do Danych osobowych (w tym dostęp, poprawianie, ograniczenie, usunięcie lub przenoszenie Danych osobowych, w zależności od sytuacji).

Jeżeli Osoba, której dane dotyczą, przekaże żądanie bezpośrednio do Podmiotu przetwarzającego, Podmiot ten niezwłocznie poinformuje Administratora i doradzi Osobie, której dane dotyczą, złożenie żądania do Administratora. Administrator jest wyłącznie odpowiedzialny za sporządzenie odpowiedzi na żądanie Osoby, której dane dotyczą.

Podmioty, którym podzlecono przetwarzanie danych osobowych. Administrator upoważnia Podmiot przetwarzający do wyznaczenia podmiotów, którym podzlecono przetwarzanie danych osobowych, jeżeli uznają to za konieczne lub właściwe w celu świadczenia usług zgodnie z niniejszą Umową powierzenia.

Przed zaangażowaniem Podmiotu, któremu podzlecono przetwarzanie danych osobowych, Podmiot przetwarzający przeprowadza weryfikację praktyk w zakresie bezpieczeństwa i prywatności oraz zgodności Podmiotu, któremu podzlecono przetwarzanie danych osobowych, z Przepisami o ochronie danych osobowych. Jeżeli Podmiot przetwarzający zamierza podzlecić przetwarzanie danych osobowych nowemu Podmiotowi, innemu niż spółki wymienione w sekcji „Lista Podmiotów, którym podzlecono przetwarzanie danych osobowych", Podmiot przetwarzający powiadomi o tym Administratora na piśmie (dla Administratora wystarczająca będzie wiadomość na adres(y) e-mail znajdujący(-e) się w dokumentacji księgowej Administratora), podając nazwę i lokalizację danego podmiotu, któremu podzlecono przetwarzanie danych osobowych, oraz czynności, jakie będzie wykonywać, a także umożliwi Administratorowi zgłoszenie uwag wobec zaangażowania nowego podmiotu, któremu podzlecono przetwarzanie danych osobowych, w ciągu 30 dni po powiadomieniu. W przypadku gdy Podmiot przetwarzający i Administrator nie będą w stanie dojść do porozumienia, każda ze stron może rozwiązać umowę o świadczenie usług zgodnie z Regulaminem za pisemnym wypowiedzeniem przekazanym drugiej stronie.

Lokalizacja i przekazywanie danych. Administrator zgadza się, aby Podmiot przetwarzający przechowywał i przetwarzał Dane osobowe na terytorium Rzeczypospolitej Polskiej i dowolnego innego państwa spoza EOG, w którym Podmiot przetwarzający lub dowolny spośród jego Podmiotów, którym podzlecono przetwarzanie danych osobowych, posiada obiekty dla celów świadczenia Usługi na rzecz Administratora. W państwach tych poziom ochrony Danych osobowych może nie być taki sam jak w EOG, jednak w przypadku przekazania danych Podmiot przetwarzający podejmie kroki w celu zapobieżenia przekazania Danych osobowych bez wdrożonych odpowiednich zabezpieczeń i dopilnuje, aby Dane osobowe użytkowników ze strony Administratora zgromadzone w EOG i przekazywane do innych państw były objęte taką samą ochroną, jak w EOG (zgodnie z art. 46 Ogólnego rozporządzenia UE o ochronie danych).

Lokalizacja danych Administratora będzie automatycznie wybierana na podstawie państwa podanego podczas procesu rejestracji. Domyślną lokalizacją przechowywania Danych osobowych w przypadku Administratora z Europejskiego Obszaru Gospodarczego (EOG) jest centrum danych w Irlandii. Lista centrów danych Podmiotów przetwarzających jest dostępna pod adresem help.calamari.io.

Integracje. Administrator jest w stanie uruchomić integrację Usług z aplikacjami zewnętrznymi. Uruchamiając integrację, Administrator zgadza się na przekazanie Danych osobowych aplikacji zewnętrznej zgodnie z celem integracji. Podmiot przetwarzający przekaże Administratorowi wszelkie informacje na temat charakteru integracji, w tym kategorie Danych osobowych, które mogą zostać przekazane do aplikacji zewnętrznej. Administrator jest wyłącznie odpowiedzialny za zgodność przetwarzania Danych osobowych przez aplikację zewnętrzną z Przepisami o ochronie danych osobowych – nie jest to przedmiot niniejszego dokumentu.

Usuwanie Danych osobowych. Podmiot przetwarzający umożliwi usunięcie Danych osobowych (w tym ich kopii) przetworzonych zgodnie z niniejszą Umową powierzenia. W przypadku gdy z przyczyn technicznych lub innych Podmiot przetwarzający nie będzie w stanie usunąć Danych osobowych, zastosuje on środki, aby dopilnować, by Dane osobowe zostały zablokowane przez dalszym przetwarzaniem.

Podmiot przetwarzający umożliwi Administratorowi:

(a) usunięcie rekordu jednej Osoby, której dane dotyczą, w dowolnym momencie,
(b) usunięcie wszystkich Danych osobowych po wygaśnięciu porozumienia,
(c) obsługę żądań, które mogą dotyczyć Danych osobowych.

Administrator nie będzie mógł przywrócić usuniętych Danych osobowych (na przykład z folderu „Kosz"). Podmiot przetwarzający usunie Dane osobowe ze swoich systemów i kopii zapasowych, jak tylko będzie to możliwe, maksymalnie w ciągu 90-dniowego okresu retencji danych.

Audyty

Administrator może wykonać przysługujące mu prawo do przeprowadzenia audytu technicznych i organizacyjnych środków bezpieczeństwa podjętych przez Podmiot przetwarzający na mocy Ogólnego rozporządzenia UE o ochronie danych.

W tym celu Administrator może na przykład:

- uzyskać informacje od Podmiotu przetwarzającego,
- zwrócić się do Podmiotu przetwarzającego o przedłożenie istniejącego zaświadczenia lub certyfikatu wydanego przez niezależnego eksperta lub
- za zasadnym i uprzednim porozumieniem, podczas normalnych godzin pracy i nie zakłócając działalności Podmiotu przetwarzającego, przeprowadzić na miejscu audyt działalności Podmiotu przetwarzającego lub zlecić taką kontrolę wykwalifikowanej osobie trzeciej, która nie jest konkurencją Podmiotu przetwarzającego. Przed rozpoczęciem audytu Administrator pokryje odpowiednie koszty audytu w całości na rzecz Podmiotu przetwarzającego uwzględniając koszty wewnętrzne Podmiotu przetwarzającego.

Na pisemną prośbę Administratora i w zasadnym czasie Podmiot przetwarzający dostarczy Administratorowi wszelkie informacje potrzebne do przeprowadzenia takiego audytu, w

takim zakresie, w jakim informacje te znajdują się pod kontrolą Podmiotu przetwarzającego, oraz o ile Podmiot przetwarzający może ujawnić takie informacje zgodnie z obowiązującymi przepisami, zobowiązaniem do zachowania poufności lub innym zobowiązaniem wobec osoby trzeciej.

Zmiany niniejszej Umowy

W przypadku gdy w dowolnym momencie Podmiot przetwarzający wprowadzi zmiany do niniejszej Umowy powierzenia, Podmiot przetwarzający zaktualizuje ten dokument, aby odzwierciedlić daną zmianę. Podmiot przetwarzający powiadomi Administratora na co najmniej 30 dni (lub w krótszym okresie zgodnie z obowiązującymi przepisami ustawowymi i wykonawczymi, nakazem sądowym lub wytycznymi rządowymi lub agencyjnymi) przed wejściem w życie zmian:
(a) wysyłając e-mail do Administratora lub
(b) powiadamiając Administratora poprzez interfejs użytkownika Usługi.

Techniczne i organizacyjne środki bezpieczeństwa

Infrastruktura przetwarzania. Podmiot przetwarzający utrzymuje swoje Usługi u zewnętrznych dostawców infrastruktury. Ponadto Podmiot przetwarzający utrzymuje stosunki umowne ze sprzedawcami w celu świadczenia Usługi zgodnie z Umową. Podmiot przetwarzający opiera się na umowach, politykach prywatności i programach zgodności sprzedawcy w celu ochrony danych przetwarzanych lub przechowywanych przez tych sprzedawców. Sprzedawcy utrzymują co najmniej N+1 poziom redundancji do zasilania, sieci i usługi HVAC.

Bezpieczeństwo fizyczne i środowiskowe. Podmiot przetwarzający utrzymuje swoje Usługi u wielodostępowych zewnętrznych dostawców infrastruktury w chmurze. Podmiot przetwarzający dopilnuje, aby przetwarzane dane użytkownika były przechowywane w sposób logiczny lub fizyczny osobno od wszelkich pozostałych danych przetwarzanych przez Podmiot przetwarzający. Kontrole bezpieczeństwa fizycznego i środowiskowego u dostawców infrastruktury podlegają audytowi pod kątem między innymi zgodności z SOC 2 Typ II i ISO 27001. Szczegóły są dostępne: https://aws.amazon.com/compliance/.

Bezpieczeństwo sieci. Podmiot przetwarzający korzysta z mechanizmów kontroli dostępu do sieci, które zaprojektowano w celu zapobiegania dostępowi do infrastruktury Usługi z wykorzystaniem nieautoryzowanych protokołów. Wdrożone techniczne środki bezpieczeństwa sieci różnią się w zależności od dostawców infrastruktury i obejmują zaporę ogniową (firewall) czy ochronę DDoS.

Uwierzytelnienie. Podmiot przetwarzający wdrożył jednolitą politykę ustawiania haseł dla swoich Usług i umożliwia uwierzytelnianie SSO. Użytkownicy, którzy korzystają z Usług poprzez interfejs użytkownika, muszą dokonać uwierzytelnienia przed dostępem do niepublicznych danych klienta.

Autoryzacja. Dane Administratora są przechowywane w wielodostępowym systemie przechowywania dostępnym wyłącznie poprzez interfejs użytkownika aplikacji i interfejs programistyczny. Administratorzy nie mają bezpośredniego dostępu do bazowej infrastruktury aplikacji. Model autoryzacji w ramach Usług Podmiotu przetwarzającego zaprojektowano w celu dopilnowania, aby wyłącznie właściwie przypisane osoby miały dostęp do odpowiednich funkcjonalności, widoków i opcji personalizacji.

Dostęp do API. Dostęp do publicznego API jest możliwy przy wykorzystaniu klucza API.

Uwzględnianie prywatności w fazie projektowania. Uwzględniając stan wiedzy technicznej, koszty wdrożenia i charakter, zakres, kontekst i cele przetwarzania oraz ryzyko, Podmiot przetwarzający skutecznie wdraża zasady ochrony danych w celu zintegrowania niezbędnych zabezpieczeń.

(a) usługi są objęte ochroną przed atakami takimi jak wstrzykiwanie kodu SQL, tokeny CSRF, XSS, i zaprojektowane zgodnie z najlepszymi praktykami;

(b) są przeprowadzane przeglądy kodu przechowywanego w repozytoriach kodu źródłowego Podmiotu przetwarzającego, kontrole najlepszych praktyk i możliwych do zidentyfikowania błędów oprogramowania. Podmiot przetwarzający bazuje na wewnętrznym i zewnętrznym doświadczeniu branżowym, aby dopilnować, by kod źródłowy był czytelny i łatwy do utrzymania.
(c) Podmiot przetwarzający wdrożył zestaw testów automatycznych w celu weryfikacji jakości kodu.

Zapora ogniowa (firewall) i antywirus. Podmiot przetwarzający wdraża odpowiednią zaporę ogniową (firewall), oprogramowanie i technologie antywirusowe, przeciwko programom szpiegującym i inne przeciwko szkodliwemu oprogramowaniu we wszystkich sieciach i systemach, jakie wykorzystuje w celu przetwarzania danych osobowych. Podmiot przetwarzający regularnie aktualizuje zaporę ogniową (firewall), oprogramowanie i technologie antywirusowe, przeciwko programom szpiegującym i inne przeciwko szkodliwemu oprogramowaniu.

Wykrywanie incydentów i monitorowanie. Podmiot przetwarzający ma wdrożony spójny proces zarządzania incydentami. Podmiot przetwarzający ciągle udoskonala ten proces w celu zredukowania wpływu incydentów, zmniejszenia ilości czasu poświęcanego na ich rozwiązanie, a przede wszystkim unikania powtarzania się tych incydentów.

Kopie zapasowa i redundancja. System infrastruktury Podmiotu przetwarzającego zaprojektowano w celu zminimalizowania wpływu spodziewanego ryzyka środowiskowego. Usługi zaprojektowano w celu ochrony, utrzymania i czynności konserwacyjnych przy utrzymaniu minimalnej przerwy. Dane Administratora są kopiowanie z wykorzystaniem standardowych metod branżowych do wielu bezpiecznych miejsc przechowywania i replikowane między różnymi strefami dostępności. Kopie zapasowe są przechowywane w bezpieczny sposób i można je odzyskać w ciągu 24 godzin.

Technologie szyfrowania. Podmiot przetwarzający wykorzystuje 256-bit owe szyfrowanie HTTPS (zwane również połączeniem SSL lub TLS). W ramach Usług Podmiot przetwarzający wspiera wymianę kluczy kryptograficznych Diffie Hellman podpisanych przez RSA. Te metody pozwalają chronić ruch internetowy oraz minimalizować wpływ zagrożenia ataków na zabezpieczenia kryptograficzne. Miejsca przechowywania danych są automatycznie szyfrowane aby chronić dane Klient w spoczynku.

Ciągłość działalności. Podmiot przetwarzający replikuje dane pomiędzy różnymi systemami i lokalizacjami, aby chronić dane przez przypadkowym usunięciem lub utratą. Podmiot przetwarzający zaprojektował oraz regularnie planuje i testuje programy przywracania ciągłości działalności i przywracania po awarii.

Bezpieczeństwo osobiste. Personel Podmiotu przetwarzającego jest zobowiązany prowadzić działalność zgodnie ze swoimi wytycznymi w zakresie poufności, etyki biznesowej, odpowiedniego użytkowania i standardów zawodowych. Podmiot przetwarzający może dokonać zasadnego i odpowiedniego sprawdzenia informacji i danych o osobie w zakresie prawnie dopuszczalnym i zgodnie z lokalnie obowiązującym prawem pracy i wymogami

ustawowymi. Personel jest zobowiązany do podpisania umowy o zachowanie poufności i musi potwierdzić otrzymanie i przestrzeganie polityki prywatności i zachowania poufności Podmiotu przetwarzającego.

Część pracowników Podmiotu przetwarzającego ma dostęp do danych Administratora poprzez kontrolowany interfejs. Celem udzielenia części pracowników dostępu jest skuteczne wsparcie dla klienta, rozwiązywanie ewentualnych problemów, wykrywanie i reagowanie na incydenty związane z bezpieczeństwem oraz wdrażanie ochrony danych. Dostęp jest tymczasowy i jest udzielony poprzez żądania „w czasie rzeczywistym”; wszystkie tego rodzaju żądania są rejestrowane.

W przypadku pytań dotyczących wdrażania technicznych i organizacyjnych środków bezpieczeństwa prosimy o kontakt: dpo@calamari.io.

Lista podmiotów, którym podzlecono przetwarzanie danych osobowych

Podmiot, któremu podzlecono przetwarzanie danych osobowych	Cel	Lokalizacja	Strona internetowa
Amazon Web Services, Inc.	Dostawca infrastruktury, dostawca usługi e-mail	USA, Irlandia, Singapur, Wielka Brytania	https://aws.amazon.com/
Google, Inc.	Dostawca usługi e-mail, produkt analityczny	USA	https://www.google.com/analytics/ https://gsuite.google.com
Intercom, Inc.	Dostawca komunikacji przez czat	USA	https://www.intercom.com
HubSpot, Inc.	Dostawca CRM	USA	https://www.hubspot.com
Slack Technologies, Inc.	Komunikacja zespołu wsparcia	USA	https://slack.com
Tawk.to Inc.	Dostawca komunikacji przez czat	USA	https://www.tawk.to
The Rocket Science Group, LLC	Dostawca usługi e-mail	USA	https://mailchimp.com
PayPal (Europe) S.a.r.l et Cie, S.C.A	Dostawca płatności	Luksemburg	https://www.paypal.com/
PayLane sp. z o.o	Dostawca płatności	Polska	http://paylane.com
OneSignal	Mobile notifications	USA	https://onesignal.com

W imieniu Klienta:

Imię i nazwisko:
Stanowisko: _____
Podpis: _____

W imieniu Calamari:

Imię i nazwisko: Hubert Lisek
Stanowisko: Członek zarządu
Podpis: Hubert Lisek