

Polityka prywatności

GX CONTROL to aplikacja mobilna, oferowana jako produkt uzupełniający dla urządzeń komunikacyjnych GSM / GPRS o nazwie **GSM-X** i **GPRS-A**. Została stworzona przez firmę **SATEL Sp. z o.o.** w celu dostarczenia naszym **Klientom** użytecznej i nowoczesnej aplikacji klienckiej, oferującej bezpieczny dostęp, zdalne sterowanie i wizualizację stanu urządzenia komunikacyjnego GSM zainstalowanego w obiekcie Klienta.

Aplikacja, dostarczana bezpłatnie przez firmę SATEL Sp. z o.o., jest przeznaczona do użytku na zasadzie "tak jak jest".

Niniejsza strona internetowa zawiera informacje o **polityce prywatności** SATEL Sp. z o.o. dla naszych **Klientów**, którzy zdecydowali się na korzystanie z naszej aplikacji. Polityka prywatności jest również dostępna w aplikacji mobilnej GX CONTROL.

Podjęcie decyzji o korzystaniu z naszej aplikacji oznacza wyrażenie zgody na zbieranie i wykorzystywanie przez nas informacji związanych z niniejszą polityką prywatności. **Informacje**, które zbieramy służą dostarczaniu i udoskonalaniu aplikacji. Informacji o Klientach nie udostępniamy nikomu, ani nie używamy do żadnych innych celów poza opisanymi w niniejszej polityce prywatności.

Gromadzenie i wykorzystywanie informacji

Podjęcie decyzji o korzystaniu z naszej aplikacji do uzyskania zdalnego połączenia i wizualizacji stanu urządzenia komunikacyjnego użytkownika oznacza zgodę na inicjalizację aplikacji klienckiej z użyciem następujących informacji: numeru **IMEI** wbudowanego modułu GSM, **identyfikatora** urządzenia komunikacyjnego i **hasła użytkownika** do konta użytkownika w jego urządzeniu komunikacyjnym (*). Taki zestaw danych jest wprowadzany do aplikacji i przechowywany lokalnie w danym urządzeniu w zasobach aplikacji. Jest on wystarczający do nawiązania połączenia z urządzeniem komunikacyjnym użytkownika.

(*) **Objaśnienia:**

- Numer **IMEI** to międzynarodowy identyfikator urządzenia mobilnego, określający moduł telefoniczny GSM wbudowany w nasze urządzenie komunikacyjne. IMEI służy do identyfikacji urządzenia użytkownika w sieci GSM i w naszym systemie. Numer IMEI jest podany w formie jawnej na etykiecie modułu telefonicznego GSM.
- **Identyfikator** urządzenia komunikacyjnego jest generowany przez nasze serwery i przypisywany do urządzenia podczas żądania i zestawiania połączenia między urządzeniem komunikacyjnym a serwerem. Identyfikator jest przechowywany w sposób zabezpieczony. Identyfikator można pobrać za pomocą funkcji użytkownika dostępnych w urządzeniu komunikacyjnym po prawidłowym uwierzytelnieniu użytkownika.
- **Hasło użytkownika** jest znane tylko danemu użytkownikowi i rozpoznawane przez jego urządzenie komunikacyjne.

Uwaga: SATEL Sp. z o.o. nie posiada kompletnego zestawu danych, które pozwoliłyby na połączenie z urządzeniem komunikacyjnym użytkownika. Po stronie Klienta powyższy zestaw danych jest przechowywany w zasobach aplikacji jego urządzenia. Dzięki dodatkowej funkcji, którą wprowadziliśmy dla naszych Klientów, możliwa jest weryfikacja dostępu do danej instancji aplikacji za pomocą hasła dodatkowego, które można zdefiniować w aplikacji.

Komunikacja typu "end-to-end" pomiędzy urządzeniem komunikacyjnym użytkownika a klientem (klientami) aplikacji mobilnej jest realizowana za pośrednictwem sieci, z wykorzystaniem bezpiecznych usług transmisji danych hostowanych przez kilka serwerów należących do SATEL Sp. z o.o.

Nawiązanie komunikacji typu end-to-end oznacza ciągłą transmisję zabezpieczonych danych z urządzenia komunikacyjnego do aplikacji Klienta w celu wymiany konfiguracji urządzenia komunikacyjnego i uzyskania informacji o stanie urządzenia komunikacyjnego za pomocą funkcji sprawdzania stanu systemu, sprawdzania stanu wejść, sprawdzania stanu wyjść, przeglądania awarii bieżących i przeglądania wszystkich zdarzeń systemowych.

SATEL Sp. o.o. nie zbiera żadnych danych związanych z komunikacją typu "end-to-end". Dane są przechowywane tylko w urządzeniu komunikacyjnym Klienta i w aplikacji mobilnej. Nasze serwery reprezentują jedynie warstwę transportową.

Decyzja użytkownika o aktywacji powiadomień PUSH w kliencie aplikacji oznacza zgodę na pobieranie przez nas identyfikatora urządzenia, na którym aplikacja jest zainstalowana, i wykorzystywanie go do świadczenia usługi powiadomień PUSH. Tokeny oznaczające instancje korzystania z usługi PUSH przez aplikację są przechowywane na naszych serwerach. Konfiguracja usługi powiadomień PUSH jest przechowywana w pamięci podręcznej aplikacji. Przy pomocy tych danych SATEL Sp. z o.o. nie jest w stanie zidentyfikować klienta.

Aby ułatwić import danych potrzebnych do inicjacji połączenia z urządzeniem komunikacyjnym użytkownika, nasza aplikacja korzysta z kodów QR. Ta sama funkcja służy do eksportu danych z urządzenia komunikacyjnego do innej instancji aplikacji użytkownika na innym urządzeniu.

Decyzja użytkownika o korzystaniu z naszej aplikacji do skanowania kodu QR i importu danych urządzenia komunikacyjnego za pomocą kodu QR oznacza zgodę na korzystanie z kamery jego urządzenia. Należy zwrócić uwagę, że nasza aplikacja używa kamery wyłącznie do odczytu kodu QR.

Dane użytkownika przechowywane w kodzie QR nie są prezentowane w sposób jawny. Kod QR jest generowany raz w czasie sesji wymiany i chroniony kluczem sesji. Klucz sesji jest zdefiniowany przez użytkownika i nie jest wymieniany w naszej aplikacji. Podczas odczytu kodu QR za pomocą aplikacji na urządzeniu docelowym użytkownik jest proszony o podanie dokładnego klucza sesji.

Nasza aplikacja nie korzysta z usług stron trzecich mogących zbierać informacje służące do identyfikacji użytkownika. Nasza aplikacja nie wykorzystuje i nie gromadzi żadnych danych, które mogą być uznane za wrażliwe.

Dane rejestru zdarzeń i analiza danych

Podjęcie decyzji o korzystaniu z naszej aplikacji oznacza zgodę na stosowanie technik analitycznych firmy **Crashlytics** (część firmy Fabric, która została nabyta przez Google). Aby dowiedzieć się więcej o polityce prywatności Crashlytics, należy odwiedzić stronę: <http://try.crashlytics.com/terms/>

Narzędzia te stosujemy do zbierania anonimowych danych, aby lepiej zrozumieć sposób w jaki użytkownik korzysta z naszej aplikacji. Dzięki nim dowiadujemy się jak ulepszyć naszą aplikację i które z jej funkcji są wykorzystywane przez użytkownika. Dostarczają nam one również ogólnych informacji o tym, gdzie na świecie nasza aplikacja jest wykorzystywana i jakiej wersji językowej nasi Klienci używają.

Informujemy, że w przypadku wystąpienia jakiegokolwiek błędu podczas pracy użytkownika z aplikacją, technika Crashlytics umożliwia przetwarzanie raportów o błędach zapisanych w rejestrze zdarzeń danego urządzenia. Dane dziennika mogą zawierać np. nazwę urządzenia, wersję systemu operacyjnego, wersję aplikacji, czas i datę użycia aplikacji. Dane rejestru zdarzeń są zbierane wyłącznie po to, aby umożliwić nam rozwój i doskonalenie naszej aplikacji.

Pliki typu "cookie"

Pliki typu cookie to pliki z niewielką ilością danych, które mogą zawierać anonimowy niepowtarzalny identyfikator. Są one przesyłane do przeglądarki Klienta z odwiedzanej przez niego strony internetowej i przechowywane w pamięci wewnętrznej urządzenia Klienta.

Strona internetowa podana w naszej aplikacji mobilnej używa cookies w celu gromadzenia informacji i poprawy jakości usług. Użytkownik ma możliwość zaakceptowania lub odrzucenia cookies, oraz dowiedzenia się kiedy plik cookie jest wysyłany do komputera Klienta. W przypadku odrzucenia naszych plików cookie, niektóre części naszego serwisu mogą być dla użytkownika niedostępne.

Bezpieczeństwo

Cenimy sobie zaufanie Klientów dostarczających nam dane, o których mowa w niniejszej Polityce Prywatności, dlatego staramy się stosować komercyjnie akceptowalne środki ochrony. Należy jednak pamiętać, że żadna metoda przesyłu danych przez Internet ani ich elektronicznego przechowywania nie jest w 100% bezpieczna i niezawodna, nie możemy więc zagwarantować ich całkowitego bezpieczeństwa.

Linki do innych stron

Nasza Aplikacja zawiera łącza URL wyłącznie do stron związanych z firmą SATEL Sp. o.o.

Zmiany w niniejszej Polityce prywatności

Nasza Polityka Prywatności może być od czasu do czasu aktualizowana. Z tego względu zalecamy okresowe śledzenie niniejszej strony internetowej pod kątem ewentualnych zmian. O wszelkich zmianach będziemy informować użytkowników poprzez opublikowanie na niej nowej Polityki Prywatności. Zmiany wchodzi w życie natychmiast po ich zamieszczeniu na niniejszej stronie.

Kontakt

W przypadku jakichkolwiek pytań lub sugestii dotyczących naszej polityki prywatności, prosimy o kontakt:

W razie jakichkolwiek pytań lub sugestii dotyczących naszej Polityki prywatności, prosimy o niezwłoczny kontakt pod adresem:

SATEL Sp. z o.o.
ul. Budowlanych 66
80-298 Gdańsk, Poland
satel@satel.pl

Made to Protect
<http://www.satel.eu/>

Privacy Policy

GX CONTROL is a mobile application and supplementary product offered for GSM / GPRS communication devices called **GSM-X** and **GPRS-A**. It was created by **SATEL Sp. z o.o.**, to provide useful and modern application client, to our **Customers**, offering: secure access, remote control and visualization of the state of the GSM communication device installed in Customer's premises.

The **Application** is provided by SATEL Sp. z o.o at no cost and is intended for use as is.

This page is used to inform our **Customers** regarding our **Privacy Policy** if anyone decided to use our Application. The Privacy Policy is also accessible at GX CONTROL mobile application.

If you decide to use our Application, then you agree to the collection and use of information in relation with this policy. The **Information** that we collect are used for providing and improving our Application. We are not using or sharing customer's information with anyone except as described in this Privacy Policy.

Information Collection and Use

If you decide to use our Application to achieve remote connection and visualization of the state of your communication device, then you agree to initialize the application client with the following information: **IMEI** of embedded GSM module, **ID** of communication device and the **User Password** representing the user account in your communication device (*). This set of data is entered in Application and stored in Application's resources, locally on your device. This set of data is enough to establish connection with your communication device.

(* *Details:*

- **IMEI** is an international mobile equipment identifier representing GSM phone module embedded in our communication device. IMEI is used to identify your device in the GSM network and in our system. IMEI is presented in clear on the label of GSM phone module.
- **ID** of communication device is generated by our servers and assigned to the device while requesting and initializing the connection between communication device and server. ID is stored in protected manner. ID can be retrieved using user functions available in the communication device upon valid authentication of the user.
- **User password** is only known to you and your communication device

Note: SATEL Sp. z o.o. does not have complete set of data which would allow to connect to your communication device. On Customer's side, above set of data is stored in application's resources on your device. Knowing that we implemented additional feature for our customers: An access to your instance of Application can be verified with additional password, which can be defined in Application.

End-to-end communication between your communication device and mobile Application client(s) is realized over the network with the use of secured transport services hosted by several servers. The servers belongs to SATEL Sp. z o.o.

Established End-to-end communication means continuous transportation of secured data from communication device to customer's Application to exchange configuration of the communication device and to get the state of communication device through the following functionalities: checking system status, checking input status, checking output status, viewing current troubles, viewing all system events.

SATEL Sp. z o.o. does not collect any data related with End-to-end communication. The data is only kept in customer's communication device and mobile Application. Our servers are only representing transport layer.

If you decide to activate PUSH messaging in Application client, then you agree that identifier of your device, on which the Application is installed, will be collected and used by us to provide PUSH messaging service. Tokens representing instances of Applications using PUSH service are stored in our servers. The configuration of PUSH messaging service is stored in Application's cache. With this data SATEL Sp. z o.o. is not able to identify the customer.

Our Application is using QR codes to ease the import of data, needed for initializing the connection with your communication device. The same functionality is used to export the data of communication device to other instance of your Application, on another device.

If you decide to use our Application to scan QR code and to import communication device's data via QR code, then you agreed to use your device's camera. Note that our Application uses camera only for QR code scanning.

The user data stored in QR code is not presented in clear. The QR code is generated once per exchange session and protected with session key. Session key is defined by the user and is not exchanged within our Application. While reading the QR code with Application on destination device, you will be prompted to enter exact session key.

Our Application does not use third party services that may collect an information used to identify you. Our Application does not use and does not collect any data which could be assessed as sensitive.

Log Data & Analytics

If you decide to use our Application, then you agree that the following analytics technologies are in use: **Crashlytics** (part of Fabric, which has been acquired by Google). To learn more about Crashlytics's privacy policy, visit: <http://try.crashlytics.com/terms/>

We use these technologies to collect anonymous data to help us understand how you use our Application. These tools help us learn how to make our Application better in use. These technologies can tell us what functions of our Application you are using. They also provide us with general information about where in the world our Application is used and what language version our customers are using.

We want to inform you that whenever you use our Application, in case of an error in the Application, Crashlytics can process the error reports stored as Log Data on your device. This Log Data may include information such as: Device name, Operating system version, Application version, the time and date of use of Application. The Log Data is only collected to allow us to lead development and improvement processes for our Application.

Cookies

Cookies are files with small amount of data which may include an anonymous unique identifier. These are sent to customer browser from the website that you visit and are stored on Customer device's internal memory.

Our web site which is referenced in our mobile Application is using cookies to collect information and to improve our Services. You have the option to either accept or refuse these cookies, and know when a cookie is being sent to Customer computer. If you choose to refuse our cookies, you may not be able to use some portions of our Service.

Security

We value Customer trust in providing us the data described above in this Privacy Policy, thus we are striving to use commercially acceptable means of protecting it. But remember that no method of transmission over the internet, or method of electronic storage is 100% secure and reliable, and we cannot guarantee its absolute security.

Links to Other Sites

Our Application contains url links only to sites related with SATEL Sp. z o.o.

Changes to This Privacy Policy

We may update our Privacy Policy from time to time. Thus, you are advised to review this page periodically for any changes. We will notify you of any changes by posting the new Privacy Policy on this page. These changes are effective immediately, after they are posted on this page.

Contact Us

If you have any questions or suggestions about our Privacy Policy, do not hesitate to contact:

SATEL Sp. z o.o.

ul. Budowlanych 66

80-298 Gdańsk, Poland

satel@satel.pl

Made to Protect

<http://www.satel.eu/>

Datenschutzerklärung

GX CONTROL ist eine mobile App, die als ergänzendes Produkt für GSM/GPRS-Kommunikationsgeräte **GSM-X** und **GPRS-A** angeboten wird. Sie wurde von **SATEL Sp. z o.o.** entwickelt, um unseren **Kunden** eine nützliche und moderne Clientanwendung zur Verfügung zu stellen, die einen sicheren Zugriff, Fernsteuerung und Visualisierung des Zustands des im Kundenobjekt installierten GSM-Kommunikationsgerätes bietet.

Die **App** wird von SATEL Sp. z o.o. kostenlos zur Verfügung gestellt und ist für den Gebrauch nach dem Prinzip "wie besehen" bestimmt.

Diese Webseite enthält Informationen über die **Datenschutzerklärung** von SATEL Sp. z o.o. für unsere **Kunden**, die sich für die Nutzung unserer App entschieden haben. Die Datenschutzerklärung ist auch in der mobilen App GX CONTROL verfügbar.

Die Entscheidung, unsere App zu nutzen, bedeutet die Einwilligung dazu, dass wir Informationen im Zusammenhang mit dieser Datenschutzerklärung erheben und verwenden. Die von uns erhobenen **Informationen** werden zur Bereitstellung und Verbesserung der App verwendet. Wir geben keine Kundeninformationen an Dritte weiter und verwenden sie auch nicht für andere Zwecke als die in dieser Datenschutzerklärung beschriebenen.

Erhebung und Verwendung von Informationen

Die Entscheidung, unsere App für die Fernverbindung und Visualisierung des Zustands des Kommunikationsgerätes des Benutzers zu nutzen, bedeutet Einwilligung zur Initialisierung der Clientanwendung bei Verwendung folgender Informationen: **IMEI-Nummer** des eingebauten GSM-Moduls, **ID-Nummer** des Kommunikationsgerätes und **Benutzerkennwort** für das Konto des Benutzers in seinem Kommunikationsgerät (*). Dieses Daten-Set wird in die App eingetragen und lokal in den App-Ressourcen gespeichert. Es ist ausreichend, um Verbindung mit dem Kommunikationsgerät des Benutzers herzustellen.

(* Erläuterungen:

- **IMEI-Nummer** ist eine internationale Identitätsnummer des Mobilgerätes, die das in unser Kommunikationsgerät eingebaute GSM-Telefonmodul definiert. IMEI wird verwendet, um das Gerät des Benutzers im GSM-Netz und in unserem System zu identifizieren. Die IMEI-Nummer ist in einer öffentlichen Form auf dem Etikett des GSM-Telefonmoduls angegeben.
- **ID-Nummer** des Kommunikationsgerätes wird von unseren Servern generiert und dem Gerät zugewiesen, während die Verbindung zwischen dem Kommunikationsgerät und dem Server angefordert und hergestellt wird. Die ID-Nummer wird auf sichere Weise aufbewahrt. Die ID-Nummer kann mithilfe der im Kommunikationsgerät verfügbaren Benutzerfunktionen nach erfolgreicher Benutzerauthentifizierung heruntergeladen werden.
- **Benutzerkennwort** ist nur dem gegebenen Benutzer bekannt und wird von seinem Kommunikationsgerät erkannt.

Bemerkung: SATEL Sp. z o.o. verfügt nicht über ein vollständiges Daten-Set, das die Verbindung mit dem Kommunikationsgerät des Benutzers ermöglichen würde. Auf Kundenseite wird das oben genannte Daten-Set in den App-Ressourcen seines Gerätes aufbewahrt. Dank zusätzlicher Funktion, die wir für unsere Kunden eingeführt haben, ist es möglich, den Zugriff auf eine bestimmte Anwendungsinstanz mit einem zusätzlichen Kennwort zu verifizieren, welches in der App definiert werden kann.

Die Ende-zu-Ende-Kommunikation zwischen dem Kommunikationsgerät des Benutzers und dem Client (Clients) der mobilen Anwendung erfolgt über das Netzwerk unter Verwendung sicherer Datenübertragungsdienste, die von mehreren Servern von SATEL Sp. z o.o. gehostet werden.

Der Aufbau einer Ende-zu-Ende-Kommunikation bedeutet eine kontinuierliche Übertragung geschützter Daten von dem Kommunikationsgerät zur App des Kunden, um die Konfiguration des Kommunikationsgerätes auszutauschen und Informationen über den Zustand des Kommunikationsgerätes mithilfe folgender Funktionen zu erhalten: Überprüfung des Systemzustands, Überprüfung des Zustands von Eingängen, Überprüfung des Zustands von Ausgängen, Durchsicht laufender Störungen und Durchsicht sämtlicher Systemereignisse.

SATEL Sp. o.o. erhebt keine Daten, die mit der Ende-zu-Ende-Kommunikation zusammenhängen. Die Daten werden nur in dem Kommunikationsgerät des Kunden und in der mobilen App aufbewahrt. Unsere Server stellen nur die Transportschicht dar.

Die Entscheidung des Benutzers über Aktivierung der PUSH-Benachrichtigungen im Client der Anwendung bedeutet die Einwilligung, dass wir die ID-Nummer des Gerätes, auf welchem die App installiert ist, herunterladen und für den PUSH-Benachrichtigungsdienst verwenden können. Die Tokens, die die Instanzen der Nutzung des PUSH-Dienstes durch die App darstellen, werden auf unseren Servern aufbewahrt. Die Konfiguration des PUSH-Benachrichtigungsdienstes wird im App-Cache aufbewahrt. Mit diesen Daten ist SATEL Sp. z o.o. nicht in der Lage, den Kunden zu identifizieren.

Unsere App verwendet QR-Codes, um den Import von Daten zu erleichtern, die zur Initialisierung der Verbindung mit dem Kommunikationsgerät des Benutzers notwendig sind. Die gleiche Funktion dient zum Export der Daten aus dem Kommunikationsgerät in andere Instanz der App des Benutzers auf einem anderen Gerät.

Die Entscheidung des Benutzers, mit unserer App den QR-Code zu scannen und Daten des Kommunikationsgerätes mittels des QR-Codes zu importieren, bedeutet Einwilligung zur Nutzung der Kamera seines Gerätes. Es ist zu beachten, dass unsere App die Kamera ausschließlich zum Lesen des QR-Codes verwendet.

Die im QR-Code gespeicherten Benutzerdaten werden in nichtvertraulicher Form nicht dargestellt. Der QR-Code wird einmal während der Datenaustauschsitzung generiert und mit dem Sitzungsschlüssel geschützt. Der Sitzungsschlüssel ist vom Benutzer definiert und wird in unserer App nicht ausgetauscht. Beim Lesen des QR-Codes mithilfe der App auf dem Zielgerät wird der Benutzer gebeten, den genauen Sitzungsschlüssel einzugeben.

Unsere App verwendet keine Dienste Dritter, die die zur Identifizierung des Benutzers dienenden Informationen erheben könnten. Unsere App verwendet und erhebt keine Daten, die als sensibel angesehen werden können.

Ereignisregisterdaten und Datenanalyse

Die Entscheidung über Nutzung unserer App bedeutet Einwilligung zur Anwendung der Analysetechniken der Firma **Crashlytics** (Teil der Firma Fabric, die von Google erworben wurde). Um mehr über den Datenschutz von Crashlytics zu erfahren, besuchen Sie bitte die Seite: <http://try.crashlytics.com/terms/>

Wir verwenden diese Technologie zur Erhebung anonymer Daten, um besser zu verstehen, wie der Benutzer unsere App nutzt. Dank ihnen erfahren wir, wie wir unsere App verbessern können und welche ihrer Funktionen vom Benutzer genutzt werden. Sie geben uns auch allgemeine Informationen darüber, wo in der Welt unsere App und in welcher Sprachversion von unseren Kunden verwendet wird.

Wir möchten Sie darüber informieren, dass beim Auftreten irgendeines Fehlers bei Nutzung der App durch den Benutzer die Crashlytics-Technik die Verarbeitung der Fehlerberichte ermöglicht, die in der Logdatei des gegebenen Gerätes gespeichert sind. Die Daten der Logdatei können z.B. Gerätenamen, Betriebssystemversion, App-Version, Uhrzeit und Datum der Appnutzung enthalten. Die Logdaten werden erhoben, um uns nur zu ermöglichen, unsere App zu entwickeln und zu verbessern.

Cookies

Cookies sind Dateien mit geringer Datenmenge, die einen anonymen, einzigartigen Identifikator enthalten können. Sie werden in den Browser des Kunden aus der von ihm besuchten Webseite geschickt und im internen Speicher des Kundengerätes gespeichert.

Die in unserer mobilen App angegebene Webseite verwendet Cookies, um Informationen zu erheben und die Qualität der Dienste zu verbessern. Der Benutzer hat die Möglichkeit, Cookies zu akzeptieren oder abzulehnen und zu erfahren, wann die Cookie-Datei an den Computer des Kunden gesendet wird. Bei Ablehnung unserer Cookies können einige Teile unseres Service für den Benutzer unzugänglich sein.

Sicherheit

Wir schätzen das Vertrauen der Kunden, die uns die in dieser Datenschutzerklärung genannten Daten zur Verfügung stellen, und bemühen uns daher, kommerziell akzeptable Schutzmaßnahmen zu ergreifen. Es sollte jedoch daran erinnert werden, dass keine Methode der Übertragung von Daten über das Internet oder deren elektronischen Speicherung 100% sicher und zuverlässig ist, so dass wir keine vollständige Sicherheit garantieren können.

Links zu anderen Websites

Unsere App enthält URL Links ausschließlich zur Seiten, die mit SATEL Sp. o.o. in Zusammenhang stehen.

Änderungen in der vorliegenden Datenschutzerklärung

Unsere Datenschutzerklärung kann von Zeit zu Zeit aktualisiert werden. Wir empfehlen daher, diese Webseite regelmäßig auf eventuelle Änderungen zu überprüfen. Wir werden die Benutzer über sämtliche Änderungen durch die Veröffentlichung einer neuen Datenschutzerklärung informieren. Die Änderungen werden unmittelbar nach der Veröffentlichung auf dieser Seite wirksam.

Kontakt

Sollten Sie Fragen oder Anmerkungen zu unserer Datenschutzerklärung haben, kontaktieren Sie uns umgehend unter:

SATEL Sp. z o.o.
ul. Budowlanych 66
80-298 Gdańsk, Polen
satel@satel.pl

Made to Protect
<http://www.satel.eu/>

Informativa sulla privacy

GX CONTROL è un'applicazione mobile per i dispositivi di comunicazione **GSM / GPRS**. È stata realizzata da **SATEL Sp. z o.o.**, per fornire un applicativo utile e di facile utilizzo, offrendo: accesso sicuro, controllo remoto e visualizzazione dello stato del dispositivo di comunicazione GSM installato.

L'**applicazione** è fornita da SATEL Sp. z o.o a costo zero ed è intesa per l'uso così com'è.

Questa pagina viene utilizzata per informare in merito alla **normativa sulla privacy**, se si decide di utilizzare l'applicazione. L'informativa sulla privacy è consultabile anche dall'applicazione mobile GX CONTROL. Se si decide di utilizzare l'applicativo, si accetta la raccolta e l'utilizzo delle informazioni in relazione a questa politica. Le **informazioni** raccolte sono utilizzate per fornire e migliorare l'applicazione. Non saranno utilizzate o condivise le informazioni con terzi, ad eccezione di quanto descritto nella presente Informativa sulla privacy.

Raccolta e utilizzo delle informazioni

Se si decide di utilizzare l'applicativo per ottenere la connessione remota e la visualizzazione dello stato del dispositivo di comunicazione, si accetta di inizializzare il client dell'applicazione con le seguenti informazioni: **IMEI** del modulo GSM incorporato, **ID** del dispositivo di comunicazione e **Password Utente** che rappresenta l'account utente nel dispositivo di comunicazione (*). I dati sono inseriti nell'applicativo e archiviati nelle risorse dell'applicazione e localmente sul dispositivo. Questo set di dati è sufficiente per stabilire una connessione con il dispositivo di comunicazione.

(*) **Dettagli:**

- **IMEI:** un identificatore internazionale di apparecchiature mobili che rappresenta il modulo telefonico GSM incorporato nel dispositivo di comunicazione. L'IMEI viene utilizzato per identificare il dispositivo nella rete GSM e nel sistema. L'IMEI è presentato in chiaro sull'etichetta del modulo telefonico GSM.
- L'**ID** del dispositivo di comunicazione è generato dai server e assegnato al dispositivo durante la richiesta e l'inizializzazione della connessione tra dispositivo di comunicazione e server. L'ID è memorizzato in modo protetto. Può essere recuperato utilizzando le funzioni utente disponibili nel dispositivo di comunicazione a seguito di un'autenticazione valida dell'utente.
- La **password utente** è nota solo all'utente e al dispositivo di comunicazione

Nota: SATEL Sp. z o.o. non ha dati standardizzati che consentirebbero di connettersi al dispositivo di comunicazione. Dal lato del cliente, i dati di cui sopra sono memorizzati nelle risorse dell'applicazione sul dispositivo. Sono state implementate funzionalità aggiuntive per gli utenti: l'accesso all'applicazione può essere verificato con una password aggiuntiva, che può essere definita nell'applicativo.

La comunicazione end-to-end tra il dispositivo di comunicazione e i client dell'applicazione, è realizzata sulla rete con l'uso di servizi di trasporto protetti ospitati da diversi server. I server appartengono a SATEL Sp. z o.o.

Comunicazione end-to-end significa: trasporto continuo di dati protetti dal dispositivo di comunicazione all'applicazione del cliente, per lo scambio della configurazione del dispositivo di comunicazione e per ottenere lo stato del dispositivo di comunicazione attraverso le seguenti funzionalità: controllo dello stato del sistema, controllo dello stato dell'ingresso, controllo dello stato dell'uscita, visualizzazione dei problemi, visualizzazione di tutti gli eventi di sistema.

SATEL Sp. z o.o. non raccoglie dati relativi alla comunicazione end-to-end. I dati vengono conservati solo nel dispositivo di comunicazione del cliente e nell'applicazione. I server rappresentano solo il mezzo di trasporto.

Se si decide di attivare le notifiche PUSH nel client dell'applicazione, l'utente accetta che l'identificativo del dispositivo su cui è installata l'applicazione sia raccolto e utilizzato per fornire il servizio di messaggistica PUSH. I token, che rappresentano istanze di applicazioni che utilizzano il servizio PUSH, sono memorizzati nei nostri server. La configurazione del servizio di messaggistica PUSH è memorizzata nella cache dell'applicazione. Con questi dati SATEL Sp. z o.o. non è in grado di identificare il cliente.

L'applicazione utilizza codici QR per facilitare l'importazione di dati, necessari per inizializzare la connessione con il dispositivo di comunicazione. La stessa funzionalità viene utilizzata per esportare i dati del dispositivo di comunicazione su un'altra istanza dell'applicazione o su un altro dispositivo.

Se si decide di utilizzare l'applicazione per eseguire la scansione del codice QR e per importare i dati del dispositivo di comunicazione tramite codice QR, si accetta di utilizzare la fotocamera del dispositivo. Si noti che l'applicazione utilizza la fotocamera solo per la scansione del codice QR.

I dati dell'utente memorizzati nel codice QR non sono presentati in chiaro. Il codice QR viene generato una volta per sessione di scambio e protetto con chiave di sessione. La chiave di sessione è definita dall'utente e non viene scambiata all'interno dell'applicazione. Durante la lettura del codice QR con l'applicazione sul dispositivo di destinazione, sarà richiesto di immettere la chiave di sessione esatta.

L'applicazione non utilizza servizi di terzi che potrebbero raccogliere informazioni utilizzate per identificare l'utente. L'Applicazione non utilizza e non raccoglie alcun dato che possa essere valutato come sensibile.

Registro dati & Analisi

Se si decide di utilizzare la nostra Applicazione, si accetta che siano in uso le seguenti tecnologie di analisi: **Crashlytics** (parte di Fabric, che è stata acquisita da Google). Per ulteriori informazioni sulla politica sulla privacy di Crashlytics, visitare: <http://try.crashlytics.com/terms/>

Queste tecnologie sono utilizzate per raccogliere dati anonimi e per aiutarci a capire come viene utilizzata l'applicazione. Questi strumenti aiutano a capire come rendere migliore l'applicativo. Queste tecnologie aiutano a comprendere quali funzioni dell'applicazione sono utilizzate. Inoltre forniscono informazioni generali sulla geo localizzazione dell'applicativo e su quale versione linguistica è utilizzata.

S'informa che ogni volta che si utilizza l'applicazione, in caso di errore, Crashlytics elabora i rapporti di errore memorizzati come dati di registro sul tuo dispositivo. Il registro dati include informazioni quali: nome del dispositivo, versione del sistema operativo, versione dell'applicazione, ora e data di utilizzo dell'applicazione. I dati del registro sono raccolti per guidare i processi di sviluppo e miglioramento dell'applicazione.

Cookies

I cookie sono file con una piccola quantità di dati che possono includere un identificatore univoco anonimo. Questi vengono inviati al browser del cliente dal sito Web visitato e memorizzati nella memoria interna del dispositivo del cliente.

Il sito web a cui si fa riferimento nell'applicazione utilizza i cookie per raccogliere informazioni e migliorare i nostri servizi. Si ha la possibilità di accettare o rifiutare i cookie e sapere quando un cookie viene inviato al computer del cliente. Se si sceglie di rifiutare i cookie, è possibile non essere in grado di utilizzare alcune parti del servizio.

Sicurezza

Appreziamo la fiducia del cliente nel fornirci i dati sopra descritti nella presente informativa sulla privacy, pertanto ci impegniamo a utilizzare mezzi commercialmente accettabili per proteggerlo. Ricordiamo che nessun metodo di trasmissione su internet o metodo di archiviazione elettronica è sicuro e affidabile al 100% e non è possibile garantire la sua assoluta sicurezza.

Collegamenti ad altri siti

L'applicazione contiene collegamenti url solo ai siti correlati a SATEL Sp. z o.o.

Modifiche alla presente informativa sulla privacy

L'informativa sulla privacy potrebbe essere aggiornata di volta in volta. Pertanto, si consiglia di rivedere periodicamente questa pagina per eventuali modifiche. Informeremo di eventuali modifiche pubblicando la nuova informativa sulla privacy in questa pagina. I cambiamenti avranno effetto immediato, dopo che saranno stati pubblicati su questa pagina.

Contattaci

Per domande o suggerimenti sulla nostra politica sulla privacy, è possibile contattare:

SATEL Sp. z o.o.

ul. Budowlanych 66

80-298 Gdańsk, Poland

satel@satel.pl

Made to Protect

<http://www.satel.eu/>

Privacy beleid

GX CONTROL is een mobiele applicatie en een aanvullend product dat wordt aangeboden voor GSM / GPRS communicatie apparaten genoemd, **GSM-X** en **GPRS-A**. Het is gemaakt door **SATEL Sp. z o.o.**, om een bruikbare en moderne applicatie te bieden aan onze **klanten**, met beveiligde toegang, afstandsbediening en status visualisatie van het GSM communicatie apparaat, welke bij de klant geïnstalleerd is.

De **applicatie** wordt kosteloos geleverd door SATEL Sp. z o.o

Deze pagina wordt gebruikt om onze **klanten** te informeren over ons **privacy beleid** als iemand beslist om onze applicatie te gebruiken. Het privacy beleid is ook toegankelijk via de mobiele GX CONTROL applicatie.

Als u besluit om onze applicatie te gebruiken, stemt u in met het verzamelen en gebruiken van informatie in verband met dit beleid. De **informatie** die we verzamelen, wordt gebruikt voor het leveren en verbeteren van onze applicatie. We gebruiken of delen geen klantgegevens met iemand, behalve zoals beschreven in dit **privacy beleid**.

Informatie verzamelen en gebruiken

Als u besluit onze applicatie te gebruiken, om een externe verbinding tot stand te brengen en de status van uw communicatie apparaat te visualiseren, gaat u ermee akkoord dat de applicatie de volgende informatie mag initialiseren: **IMEI** van ingebouwde GSM module, **ID** van het communicatie apparaat en het **gebruiker paswoord** welke de gebruikersaccount in uw communicatie apparaat voorstelt (*). Deze gegevens worden ingevoerd in de applicatie en opgeslagen in de bronnen van de applicatie, lokaal op uw apparaat. Deze set aan gegevens is voldoende om verbinding te maken met uw communicatie apparaat.

(*) *Details:*

- Het **IMEI** nummer is een internationale identificatienummer voor mobiele apparatuur en vertegenwoordigt bij ons de GSM telefoonmodule die ingebouwd is in ons communicatie apparaat. Het IMEI nummer wordt gebruikt om uw apparaat te identificeren in het GSM netwerk en in ons systeem. Het IMEI nummer wordt duidelijk weergegeven op het label van de GSM telefoonmodule.
- het **ID** nummer van het communicatie apparaat wordt gegenereerd door onze servers en wordt toegewezen aan het apparaat tijdens het aanvragen en initialiseren van de verbinding tussen communicatie apparaat en de server. Het ID nummer wordt op een beveiligde manier opgeslagen. Het ID kan worden opgehaald met behulp van gebruikersfuncties die beschikbaar zijn in het communicatie apparaat na geldige verificatie van de gebruiker.
- Het **gebruiker paswoord** is alleen bij u en uw communicatie apparaat bekend.

Opmerking: SATEL Sp. z o.o. heeft geen gegevens waarmee verbinding gemaakt kan worden met uw communicatie apparaat. Aan de kant van de klant worden bovenstaande gegevens opgeslagen in de bronnen van de applicatie op uw apparaat. Wetende dat we extra functies hebben geïmplementeerd voor onze klanten: toegang tot uw exemplaar van de applicatie kan worden geverifieerd met een extra paswoord, welke gedefinieerd kan worden in de applicatie.

End-to-end communicatie tussen uw communicatie apparaat en mobiele applicatie(s) wordt gerealiseerd via het netwerk met behulp van beveiligde transportdiensten, die worden gehost door verschillende servers. Deze servers zijn eigendom van SATEL Sp. z o.o.

Gevestigde end-to-end communicatie betekent; continu transport van beveiligde gegevens van het communicatie apparaat naar de applicatie van de klant om de configuratie van het communicatie apparaat uit te wisselen en om de status van het communicatie apparaat via de volgende functies te verkrijgen: controleren systeem status, controleren ingang status, controleren uitgang status, storingen bekijken, alle systeem gebeurtenissen bekijken.

SATEL Sp. z o.o. verzamelt geen gegevens gerelateerd aan End-to-end communicatie. De gegevens worden alleen bewaard in het communicatie apparaat en in de mobiele applicatie van de klant. Onze servers zijn enkel en alleen een transport laag.

Als u besluit om PUSH berichten in de applicatie te activeren gaat u ermee akkoord dat het ID van uw apparaat, waarop de toepassing geïnstalleerd is, door ons verzameld en gebruikt wordt om de PUSH berichtenservice te bieden. Tokens die exemplaren van de applicaties vertegenwoordigen en de PUSH service gebruiken, worden opgeslagen op onze servers. De configuratie van de PUSH berichtenservice wordt opgeslagen in de cache van de applicatie. Met deze gegevens kan SATEL Sp. z o.o. de klant niet identificeren.

Onze applicatie gebruikt QR-codes om het importeren van gegevens te vereenvoudigen, wat nodig is voor het initialiseren van de verbinding met uw communicatie apparaat. Dezelfde functionaliteit wordt gebruikt om de gegevens van een communicatie apparaat naar een ander applicatie exemplaar op een ander apparaat te exporteren.

Als u besluit onze applicatie te gebruiken om de QR-code te scannen en de gegevens van het communicatie apparaat via de QR-code te importeren, stemt u ermee in de camera van uw apparaat te gebruiken. Onthoud dat onze applicatie de camera alleen gebruikt voor het scannen van QR-codes.

De gebruikersgegevens die zijn opgeslagen in de QR-code worden niet weergegeven. De QR-code wordt eenmaal per uitwisseling-sessie gegenereerd en met een sessie sleutel beveiligd. De sessie sleutel wordt gedefinieerd door de gebruiker en wordt niet uitgewisseld binnen onze applicatie. Tijdens het lezen van de QR-code met de applicatie op het bestemmingsapparaat, wordt u gevraagd om de exacte sessie sleutel in te voeren.

Onze applicatie maakt geen gebruik van services van derden die mogelijk informatie verzamelen en gebruikt kunnen worden om u te identificeren. Onze applicatie gebruikt en verzamelt geen gegevens die als gevoelig kunnen worden beoordeeld.

Loggegevens & Analyses

Als u besluit onze applicatie te gebruiken, gaat u ermee akkoord dat de volgende analyse technologieën worden gebruikt: **Crashlytics** (onderdeel van Fabric, dat overgenomen is door Google). Ga voor meer informatie over het privacy beleid van Crashlytics naar: <http://try.crashlytics.com/terms/>

We gebruiken deze technologieën om anonieme gegevens te verzamelen die ons helpen te begrijpen hoe u onze applicatie gebruikt. Deze tools leren ons hoe we de applicatie kunnen verbeteren. Deze technologieën kunnen ons vertellen welke functies u van onze applicaties gebruikt. Ze geven ons ook algemene informatie over waar onze applicatie wordt gebruikt en welke taal versie onze klanten gebruiken.

We willen u erop wijzen dat wanneer u onze applicatie gebruikt en in geval van een fout in de applicatie, Crashlytics deze foutrapporten kan verwerken welke opgeslagen zijn als loggegevens op uw apparaat. Deze loggegevens kunnen informatie bevatten zoals: apparaat naam, versie besturingssysteem, applicatie versie, de tijd en datum wanneer de applicatie gebruikt werd. De loggegevens worden alleen verzameld om ons in staat te stellen om ontwikkelings- en verbeteringsprocessen voor onze applicatie te maken.

Cookies

Cookies zijn bestanden met een kleine hoeveelheid gegevens die een anonieme unieke identificatie kunnen bevatten. Deze worden verzonden naar de browser van de klant vanaf de website die u bezoekt en worden opgeslagen op het interne geheugen van het apparaat van de klant.

Onze website, waarnaar wordt verwezen in onze mobiele applicatie, gebruikt cookies om informatie te verzamelen en onze services te verbeteren. U hebt de mogelijkheid deze cookies te accepteren of te weigeren en te weten wanneer een cookie naar de computer van de klant wordt verzonden. Als u ervoor kiest om onze cookies te weigeren, kunt u mogelijk sommige delen van onze service niet gebruiken.

Beveiliging

We waarderen het vertrouwen van de klant in het verstrekken van de hierboven beschreven gegevens in dit privacy beleid en we streven ernaar om commercieel aanvaardbare middelen te gebruiken om dit te beschermen. Maar vergeet niet dat geen enkele transmissie methode via internet of elektronische opslag 100% veilig en betrouwbaar is en we kunnen de absolute veiligheid ervan niet garanderen.

Links naar andere sites

Onze applicatie bevat URL-links alleen naar sites gerelateerd aan SATEL Sp. z o.o.

Wijzigingen in dit privacy beleid

We kunnen ons privacy beleid van tijd tot tijd bijwerken, daarom wordt u geadviseerd deze pagina regelmatig te controleren op eventuele wijzigingen. We zullen u op de hoogte brengen van eventuele wijzigingen door het nieuwe privacy beleid op deze pagina te plaatsen. Deze wijzigingen worden onmiddellijk van kracht, nadat ze op deze pagina zijn geplaatst.

Neem contact met ons op

Als u vragen of suggesties heeft over ons privacy beleid, aarzel dan niet om contact op te nemen met:

SATEL Sp. z o.o.
ul. Budowlanych 66
80-298 Gdańsk, Poland
satel@satel.pl

Made to Protect

<http://www.satel.eu/>