



OTTO –usługi cyfrowe: w jaki sposób firma Busch Vacuum Solutions bezpiecznie przetwarza Twoje dane.

Firma Busch będzie bezpiecznie przetwarzała dane każdego klienta w ramach umowy OTTO – usługi cyfrowe.

Jakie dane będą gromadzone?

Jedynymi danymi gromadzonymi przez firmę Busch są nazwa i adres firmy, dane osobowe użytkownika (adres e-mail, numer telefonu i adres pocztowy) oraz nieprzetworzone dane z czujników pompy próżniowej (temperatura, ciśnienie wylotowe, ciśnienie wlotowe itp.).

W jaki sposób gromadzone są dane z mojej pompy próżniowej?

Sygnały są odbierane za pośrednictwem czujników zainstalowanych w pompie próżniowej. Zostają one w bezpieczny sposób przeniesione do chmury firmy Busch. Dane są przechowywane w chmurze firmy Busch do celów analitycznych.

Jeśli nie uzgodniono inaczej, OTTO – usługi cyfrowe nie wymagają dostępu do sieci Wi-Fi klienta.

Dlaczego dane są przesyłane do chmury firmy Busch?

Po bezpiecznym zapisaniu danych w naszej chmurze specjalnie opracowane algorytmy analizują nieprzetworzone dane z pompy próżniowej w celu dostarczenia ostrzeżeń, alarmów, danych wejściowych do konserwacji zapobiegawczej, kluczowych wskaźników wydajności i historycznych danych dotyczących pomp.

Dane są gromadzone wyłącznie w tym celu.

W jaki sposób zabezpieczone jest przesyłanie danych?

Chmura Busch działa w oparciu o usługę Microsoft Azure. W celu zapewnienia wysokiego poziomu bezpieczeństwa pracujemy w chmurze wyłącznie dla Busch Vacuum Solutions.

Certyfikowany IoT Box firmy Busch jest skonfigurowany z usługą DPS (Device Provisioning Service) Azure IoT Hub, która obsługuje urządzenia IoT w zakresie łączności.

Dane z monitorowanej pompy próżniowej są przesyłane do chmury Busch za pomocą bezpiecznych kluczy symetrycznych (tokenów SAS) i szyfrowanych pakietów Jason przy użyciu uwierzytelniania z certyfikatem TLS dostarczanego przez DigiCert. Do transmisji danych służy protokół MQTT.



Pakiety mają niepowtarzalny numer identyfikacyjny. Gdy dane docierają do chmury zabezpieczonej przez rozwiązanie Azure Defender, numer identyfikacyjny służy do kontroli, czy przychodzące dane mają autoryzację. Po przeprowadzeniu kontroli bezpieczeństwa dane zostają bezpiecznie zapisane w chmurze.

W celu uzyskania dodatkowych informacji na temat używanego certyfikatu TLS (DigiCert Global G2 Root) kliknij tutaj: (<https://techcommunity.microsoft.com/t5/internet-of-things-blog/azure-iot-tls-critical-changes-are-almost-here-and-why-you/ba-p/2393169>)

W celu uzyskania dodatkowych informacji na temat rozwiązania Azure Defender kliknij tutaj: <https://azure.microsoft.com/en-us/products/iot-defender/#overview>

Czy mogę w dowolnym momencie przerwać gromadzenie danych?

Jeśli nie uzgodniono inaczej, umowa może zostać rozwiązana przez każdą ze stron w dowolnym momencie w formie pisemnej, z zachowaniem miesięcznego okresu wypowiedzenia do końca miesiąca kalendarzowego.

Rozwiązanie umowy obejmuje również wypowiedzenie konta użytkownika i w stosownych przypadkach wszystkich kont użytkownika udostępnionych klientowi.

Prawo do rozwiązania umowy z ważnego powodu bez zachowania okresu wypowiedzenia pozostaje nienaruszone.