



OTTO - Digital Services: come Busch Vacuum Solutions gestisce in modo sicuro i vostri dati.

Busch si occuperà della gestione in sicurezza di tutti i dati dei clienti per l'intero corso dei loro contratti OTTO - Digital Services.

Quali dati saranno raccolti?

Gli unici dati che Busch raccoglierà sono il nome e l'indirizzo della società, i dati personali dell'utente (indirizzo e-mail, numero di telefono e indirizzo postale) e i dati non elaborati del sistema a sensori della pompa per vuoto (temperatura, pressione di scarico, pressione in aspirazione ecc.).

Come vengono raccolti i dati dalla mia pompa per vuoto?

I segnali vengono raccolti tramite i sensori installati sulla pompa per vuoto, per essere poi trasferiti in sicurezza nel cloud Busch. I dati vengono archiviati nel cloud Busch per l'analisi.

Se non diversamente concordato, gli OTTO - Digital Services non richiedono l'accesso alla rete Wi-Fi del cliente.

Perché i dati vengono inviati al cloud Busch?

Una volta che i dati sono archiviati in sicurezza nel nostro cloud, algoritmi appositamente sviluppati analizzano i dati grezzi della pompa per vuoto, per fornire avvisi, allarmi, input di manutenzione preventiva, indicatori delle key performance e dati storici della pompa per vuoto.

I dati vengono raccolti esclusivamente per questo scopo.

Come viene protetta la trasmissione dei dati?

Il cloud Busch è fornito da Microsoft Azure. Per garantire un elevato livello di sicurezza, lavoriamo con un cloud dedicato esclusivamente a Busch Vacuum Solutions.

Busch IoT Box certificato è configurato con un DPS (Device Provisioning Service) Azure IoT Hub che supporta i dispositivi IoT per la connettività.

I dati provenienti dalla pompa per vuoto della soluzione monitorata vengono trasmessi al cloud Busch con tecnica di crittografia a chiave privata (token SAS) e pacchetti JSON crittografati, utilizzando autenticazioni dei certificati TLS di DigiCert. Per la trasmissione dei dati viene utilizzato un protocollo MQTT.



I pacchetti hanno un numero identificativo univoco. Dopo che i dati hanno raggiunto il cloud protetto da Azure Defender, il numero identificativo permette di verificare se tali dati sono autorizzati. Dopo il controllo di sicurezza, i dati vengono archiviati nel cloud.

Per ulteriori informazioni sul certificato TLS utilizzato (DigiCert Global G2 Root), cliccare qui: (<https://techcommunity.microsoft.com/t5/internet-of-things-blog/azure-iot-tls-critical-changes-are-almost-here-and-why-you/ba-p/2393169>)

Per ulteriori informazioni su Azure Defender, cliccare qui: <https://azure.microsoft.com/en-us/products/iot-defender/#overview>

Posso interrompere la raccolta di dati in qualsiasi momento?

Se non diversamente concordato, il rapporto contrattuale può essere terminato da una delle parti in qualsiasi momento utilizzando la forma scritta, con un mese di preavviso rispetto alla fine del mese di calendario.

La terminazione del rapporto contrattuale implica anche la chiusura dell'account utente e, se applicabile, di tutti gli account utente forniti per il cliente.

Resta invariato il diritto di terminazione per buona causa senza il rispetto del periodo di preavviso.