Platform & client data security policy

At LegionellaDossier, we take security seriously – both yours and ours.

Because we're a SaaS platform, we have both a duty and an obligation to safeguard your and your customers' data. This is why we've put policies in place to ensure we adhere to our industry's most stringent security guidelines.

Infrastructure & platform security

Hosting

We host our entire infrastructure and platform in the European Economic Area (EEA) in a ISO/IEC 27001 certified datacenter. We encrypt all our client-server communications and data at rest (storage). These measures include secure access for on-premise staff and full end-to-end encryption for both on-site and off-site back-ups.

Privacy & GDPR

We physically store all LegionellaDossier data within the European Economic Area (EEA) in full compliance with the EU General Data Protection Regulation (GDPR).

App communications

We secure our LegionellaDossier mobile apps in accordance with the best practices for each platform. This includes keeping both iOS and Android apps fully up to date with the latest security features and only allowing apps to communicate with the LegionellaDossier servers using SSL/TLS 1.3 encrypted channels and OAUTH tokens.

Web communications

We secure client-server communications using SSL/TLS 1.3 encryption, ensuring data is also encrypted in transit. You can verify this for yourself by checking for the 'lock' symbol and 'https' prefix in your browser's URL field.

IoT sensors

We use LoRa network technology for our Clip'R sensors and gateways. This means that communication between devices runs on LoRaWAN infrastructure, which we secure using a variety of industry standards for wireless IoT communications and chirp signals. Devices communicate with the remote server over wireless networks, using end-to-end encrypted mobile connections.

Find out more about how we encrypt all our communications.

Data storage & safety

Your data's integrity and safety are paramount, which is why we've implemented numerous safety measures:

Data access

We store customer data in our database, which remains secure during back-up and in transit.

Our employees only have access to data as part of normal operations and for customer support purposes. We've vetted every individual with access to this data and ensure they follow best practices for handling customer data.

A select group of our employees also has access to our database to ensure operational continuity. We vet these individuals even more stringently and have them sign agreements to ensure they protect all data to which they may have access for operational purposes.

Backups

We automatically backup our database every day by creating a snapshot, which allows for rapid recovery in the event of an incident.

This automated process never exposes back-ups to external or internal access except to perform a system restore. We save back-ups using encryption and store them at a secure physical location.

All the above also applies to file and document back-ups, which we perform weekly.

Disaster recovery

Our system administrators have access to all back-ups so they can restore systems to the last-known state in the event of a critical system failure. In such cases, a select group of our employees has access to customer data in order to restore system functionality.

We've also put a disaster recovery plan into place, outlining how to respond in the event of a critical failure. This plan includes several manual steps to ensure data security and rapid recovery.

Third-party data usage

LegionellaDossier never shares any customer data between customer accounts and enforces strict data segregation as part of its multi-tenancy SaaS platform policies. This means that no one can access data belonging to another customer without proper authorisation.

Third-party suppliers never have access to customer data, except those with vested business integrations. Our vested partners have access to a very limited dataset, as required for the operational functionality they provide to LegionellaDossier customers. They are not permitted to use this data for any commercial purposes.

LegionellaDossier data usage

LegionellaDossier never uses any partner or customer data for commercial purposes. We only use certain data to safeguard system operations and provide customer support and service.