GOVERNANCE & STRATEGY

AUDIT FOR INFORMATION SECURITY & GOVERNANCE STRENGTHENING

SPITEX RECHTES LIMMATTAL

Image: Spitex Rechtes Limmattal

SECURE IT GOVERNANCE AND SUSTAINABLE GOVERNANCE PRACTICES

As Spitex Rechtes Limmattal operates under a public service mandate, its measures relating to cybersecurity and data protection are regularly monitored by the Data Protection Officer of the Canton of Zurich. For this reason, Spitex Rechtes Limmattal commissioned SPIE ICS to identify potential security risks within its IT governance, and to strengthen organisational governance practices in order to continue to meet rising regulatory requirements.

DIE CHALLENGE

As a healthcare service provider with a public service mandate, Spitex Rechtes Limmattal is subject to strict legal requirements imposed by the Canton of Zurich regarding cybersecurity and the protection of patient data. The precise contractual relationships with IT service providers, the identification of potential security gaps, and the safeguarding of patient data all represent core challenges. The aim was to clarify IT service provider contracts, minimise security risks, and transparently demonstrate compliance with data protection requirements, ensuring recognition from the Data Protection Officer of the Canton of Zurich. A key focus was also on the sustainable strengthening of the client's governance practices.

Überall für alle
SPITEX
Rechtes Limmattal

Spitex Rechtes Limmattal is a non-profit organisation operating in healthcare. As a service provider with a public service mandate from the municipalities of the right bank of the Limmat, from Oberengstringen to Oetwil an der Limmat, it delivers high-quality home nursing, palliative care, and domestic support services.

Its focus is always on maintaining the quality of life and independence of its patients in their familiar home environment.

A SOLUTION AT ORGANISATIONAL AND TECHNICAL LEVEL

SPIE ICS supported Spitex Rechtes Limmattal with a comprehensive information security audit, as well as a security check and awareness training. In order to ensure the sustainability of these measures, the roles of Information Security Officer (ISO) and Data Protection Officer (DPO) were further clarified.

In addition to organisational measures, the solution also covered technical aspects: gaps in cloud security were closed, and misconfigurations in technical authentication by an IT service provider were rectified. In this process, essential security policies were developed and implemented.

> “Working with SPIE ICS helped us to clearly identify risks, sharpen responsibilities, and implement sustainable improvements in our IT governance. For us, the practical and reliable support was key.”

Emina Patokovic
Managing Director Spitex Rechtes Limmattal

PROJECT PHASES

- **Initial analysis:** Stocktaking of existing IT processes and IT service provider contracts.
- **Gap and risk analysis:** Identification of shortcomings in collaboration with IT service providers and verification of compliance with data protection regulations.
- **Action planning:** Development of specific security policies and solutions to close identified gaps.
- **Implementation:** Support in implementing organisational measures and refining the ISO and DPO roles.
- **Validation:** Review of the implemented measures by the Data Protection Officer of the Canton of Zurich.

MEASURABLE RESULTS

- **Elimination of security risks** identified within IT governance
- **Sustainable strengthening** of organisational governance practices
- **Recognition of the implemented measures** by the Data Protection Officer of the Canton of Zurich

SPIE ICS AG is your independent service partner in Switzerland for solutions in the fields of governance and information security.

Contact us to benefit from our expertise and learn more about our services and solutions:

info.ch@spie.com

spie.ch/en/governance