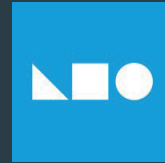
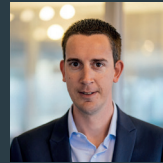


# success story



«Becoming an expert in IT security and compliance does not happen overnight. These areas, including legal and technical aspects, are very important for us; Itecor's contribution has proved to be an accelerator and a guarantee of quality».

Olivier Vanderperre, Technology & Customer Service Director



The protection of personal data is at the heart of neo technologies' Smart Metering platform and its thousands of smart meters that collect personal data from consumers. From the design phase onwards, neo technologies has ensured that it has a secure and DPA-compliant solution for the various markets.

As part of the Swiss government's Energy Strategy 2050, the Electricity Supply Ordinance requires distribution system operators (DSOs) to replace 80% of their metering systems with Smart Metering solutions by 31 December 2027. The objectives are to achieve a more accurate measurement of consumption on the network at a given time, to be able to adapt electricity production accordingly and to reduce supply risks.

As energy supply is an extremely sensitive issue, the DSOs are working closely with the federal government and the National Centre for Cyber Security.

To support its DSO customers, neo technologies has been developing a platform ("BlueWave") for several years that enables the management of smart meters developed by Landis+Gyr and GWF.

The collaboration between neo technologies and Itecor focused on the definition and implementation of the processes and organisation required to comply with the Swiss Data Protection Act (DPA).

## neo technologies

neo technologies, as a leading Swiss consulting and SAP solution provider for the energy markets, has always been very attentive to Smart Metering regulations. Since 2009, neo technologies has developed a solution (BlueWave) for the management of these smart meters with AMR technologies, which measure the consumption of electricity, heat, water and gas in detail, accurately and, if necessary, in real time.

"Itecor's added value was to directly impose an approach based on their experience in carrying out such a project. This approach made it possible to adapt to the evolution of the IT security context, in the broad sense, which changed during the course of the project. "The goal was to anticipate the changes in the DPA in order to adapt the processes and the organisation accordingly. The detailed knowledge of the law and the understanding of the context and the challenges of the platform were thus decisive: types of data, how they're used and data retention.

A data security and compliance concept are now in place. It includes a Security Officer and a Data Protection Officer to ensure the necessary governance and to implement the various regulations, as well as all the required documentation (processing register, organisation, technical documentation of IT security, etc.).

This allows Olivier Vanderperre to conclude: "We can reassure our customers about the security of our platform and guarantee them that everything is in order in terms of personal data protection. Everything has been done the way it should, despite the fact that this is something that is always evolving.

