Informasjonssikkerhet

The Infotjenester Group consists of the companies Infotjenester AS, Capitech AS, Tholin & Larsson AB and Netcompetence AB, hereafter named as **Simployer**. This page including sub pages describes how Simployer processes information securely.

Confidentiality

The companies in the Simployer Group work after best practice for the information to not be made available to persons who do not have legal access to the information. The work is based on internal risk assessments, documented routines that prevents risks and product development that has confidentiality as the most important criteria.

This is done by providing the customer with:

- secure ways of athentication
- flexible and secure role models
- privacy by design on multiple levels in the products

We also have:

- privacy as an important factor in all phases of product development
- automated and manual testing when deploying products
- training of staff in privacy and security
- 3rd party audits of our quality system

Integrity

The companies in the Simployer Group work after best practice so that can not be changed in an unauthorized or unintentional manner. The work is based on internal risk assessments, documented routines that prevents risks and product development that has integrity as an important criteria.

All customers who implement Simployer get their own dedicated customer database. Data from different customer databases is never mixed. Strict access control and role model also help ensure data integrity.

The systems use built-in and proven tools in SQL Servers and Microsoft . Net framework for data integrity.

Read more under Data Security

Availability

The companies in the Simployer Group work after best practice so that the information is available and operational at all agreed times of legal and authorized use and that the data may be transported in an agreed manner if required.

Simployer currently operates HSE systems, personnel systems, time /planning systems, learning management systems, staff / management manuals and other systems for more than 2000 customers, whereof some are among the largest companies in the Nordic. Simployer is responsible for ensuring that the systems are operational at all times, and that security and backup at all times are taken care of in the best possible way. Details are regulated in Standard Service Level Agreement (SLA), and Data Processing Agreements.

Data portability

Customer data belongs to the customer. Customers can terminate the service in accordance with agreed deadlines, and it is regulated in the SLA how Simployer will return and remove all customer data after expiration of the agreement.

Customers may at any time during the term of the agreement have its data exported to a machine readable format.

Transparency

As a customer of Simployer you know "where" your data is stored, "who" has access to data and "how" data is processed.

- **Where** : Read more about Simployer hosting providers.
- **Who has access** : After the service is established, only the customer has access to his data. Before the service is established, only the customer and trusted staff at Simployer have access to the customer's data for the purpose of assisting in the establishment of the service.
- **How is data processed**: After establishing the service, it is the customer who controls which persons should have access to the customer's data. The systems are designed to enable employers to perform their duties as an employer, and they are designed in a way that helps the customer to comply with Privacy .

On this page