Security principles

License12 is a software-as-a-service platform that places considerable emphasis on security. To achieve the high standards of security, reliability and service availability that our customers expect, we adhere to the following principles as well as the latest best practice:

1. Protecting the user
   We protect our users from the risks of mistaken identity and identity theft when they register and/or log in. We require our users to provide a text message capable telephone number or appropriate text-to-speech voice service in the country concerned. Users will each choose a secure password that he or she shall protect from unauthorised access.
2. Keeping contract data safe
   The master user (registrant) for each customer has the option of defining access groups to make certain contract data available to only a restricted circle among their designated users. We will provide master users with training in these administrative tasks, on a request basis. When for any reason a user's ability or privilege to manage their assigned account should end, their access provisions can be revoked as soon as the user's departure is made known, provided there are other users that have access to the data managed by him or her.
3. Protecting the data centre
   The data centre incorporates basic measures for preventing unauthorised access. They consist of an access control via ID-cards, an intruder alarm system, video surveillance and on-site building surveillance by a security contractor.
4. Protecting the servers
   Servers receive security updates daily. Additionally, dedicated protection mechanisms, both hardware- and software-based, are employed to prevent unauthorised access.
5. Protecting the application
   The application software undergoes regular security audits. These are based on the most up-to-date know-how of cyber-crime. Any outdated practice or other security concern thereby discovered will be addressed with appropriate measures in terms of soft- and hardware.
6. Protecting the database
   Our database is redundantly synchronised every second and remotely backed up daily. Independent of this, users may download the current state of data applicable to them in Office format. Users can thereby take charge of their own data state at any time.
7. Safeguarding payment information
   Processing of payments is done through a PCI-DSS certified provider, equivalent to protection used for online transactions in the financial sector.