Focal Point: Data Protection

Non-transparent users

Maximum data protection, maximum possibilities

The sale of data, mass surveillance, and privacy violations: with the digitalization of our world, personal data has become a gold mine for the economy and the advertising industry.

No chance of espionage

With its *connect* app, the Graz-based start-up, e.com sets a clear signal against this trend, and a clear signal in favour of data protection, and the preservation of privacy. As a social network, *connect* offers, in addition to the features of other social networks, further extras, but it will not be financed by the sale of personal data, which cannot be accessed due to the guaranteed end-to-end encryption in any case. As e.com CEO Michael Schöggl explains "Our aim was to create a data-secure, encrypted social network that, with innovative possibilities like Virtual Reality, is attractive enough for a broad target group." Although every user has the opportunity to make his or her virtual home as personal as possible, the user alone decides which areas or what information is visible to the public.

"That is solely my business."

"Our customers can decorate their virtual loft which forms the user interface of the app with their own pictures, and furnish it according to individual preferences," says Michael Schöggl, describing the individualisation possibilities of the app. For example, the loft can be furnished with furniture from various different furniture suppliers. This way, every *connect* user can express their own style without having to fear that their preferences are passed on to third parties, or misused for advertising purposes.

Full control over your own communication

It is also possible to delete sent messages or to make information accessible only for a certain amount of time; after a specified time period, the message will be deleted automatically. This way, each *connect* user can ensure that their published information does not circulate unexpectedly on the internet, or get into the wrong hands. When communicating via other messaging services using the multi-messenger in the *connect* app, however, data protection cannot be guaranteed - this is the responsibility of the respective messaging service which can continue to evaluate and pass on data at will. "We also offer a 100% secure mobile messaging service with the latest end-to-end encryption," explains Michael Schöggl. This combination ensures that encrypted and protected messages can be exchanged among *connect* users, and that users do not have to do without their contacts outside the *connect* world.