vocatus:

Data protection and data security at Vocatus

Dealing with highly sensitive data is part of our daily business. We know all too well that the confidentiality of the data that's been gathered and evaluated is very important to you. That's why we're very fastidious about data protection and data security.

As market researchers, we're subject to the strict guidelines laid down by the General Data Protection Regulation (GDPR), the Federal Data Protection Act (BDSG) and additional appropriate data protection laws, and we're regularly checked by the regulatory authorities responsible for data protection to ensure we're adhering to these rules.

As a member of the Federal Association of German Market and Social Researchers (BVM), we're furthermore obliged to respect the official guidelines on dealing with data in market and social research as published jointly by the BVM and the Association of German Market and Social Research Institutes (ADM).

Regular data protection audits

Vocatus has already undergone a number of successful data protection audits, and has repeatedly demonstrated that it enforces the most rigorous security standards when it comes to data protection. It goes without saying that we follow a strict IT security concept as set out in Art. 32 para. 1 GDPR.

Our employees' obligations with regard to data protection

Our employees undertake to maintain confidentiality and data secrecy from the moment they accept a post with us. Their first day at work includes an induction into the topic of information security and data protection, and they subsequently receive regular training about data protection questions.

Infrastructure

Within the context of market research studies, data is generally stored, processed and used exclusively on systems belonging to Vocatus AG in Germany (and not on Cloud services or the like).

The hosting of our online questionnaires takes place in a secure computer centre with comprehensive access controls, surveillance, 24/7 staffing, and areas with restricted access. The infrastructure is supported by back-up systems, and protected from external interference by state-of-the art firewalls. Communication between the client (participant's browser) and the survey servers at Vocatus is TLS-encrypted (https).The despatch of invitation emails, etc. is likewise TLS-encrypted so long as this is supported by the receiving mail system.

An internal IT team manages the company's IT infrastructure (including 24/7 monitoring with text message and email notification).

Strict password protection

All our in-house systems and files are protected against unauthorised access by a strict personalised password system. The basic principle here is that each member of staff only has access to precisely the data they actually need for their immediate work.

Data protection in the context of studies

Personal data is only used within the framework of the study that is to be conducted, is not passed on to any third parties, and is deleted by Vocatus once the study has been completed.

Information gathered about respondents within the framework of projects is only passed on in anonymised form, so that it's impossible to identify individuals. It goes without saying that our results reports also make it impossible to draw any conclusions about individuals.

Particularly in the case of employee surveys, it’s hugely important that the evaluation should be completely anonymous. Due to this, we do not report results for groups smaller than the previously agreed minimum sample size.

It's also the case with mystery and call monitoring studies that test the service quality of individual areas of the company (such as call centre, customer care, or complaint management) that we don't pass on any personal data such as staff names to the client or third parties.

When it comes to multi-client studies, each participating company receives detailed evaluations concerning their own company, while the competitors' figures are presented in anonymised form. If requested, evaluations that mention the individual company names can also be created for those participating companies that consent to this disclosure, and so long as this data is to be exclusively used for internal purposes.

Contact people

Alexander Weigmann (Board Member)
Albert Stamate (Data Protection Officer)
If you have any questions about data protection, please contact: datenschutz@vocatus.de