# 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 consultants, 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.

## 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 our projects, we use resources of the Vocatus Group (Vocatus AG and its affiliates/subsidiaries), services of Microsoft Corporation and particularly for data collection tasks, products of Qualtrics LLC; personalized data is stored, processed and used exclusively on systems in Germany and the EU. We concluded data processing agreements with all providers.

Hosting of the Vocatus IT infrastructure takes place in a secure data center 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 is TLS-encrypted (https).The transfer of invitation emails, etc. is likewise TLS-encrypted, if supported by the receiving mail system.

An internal IT team manages the Vocatus 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 unauthorized access by a strict personalized 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 surveys

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

Information gathered about respondents within the framework of projects is only passed on in anonymized 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.

## Contact people

Alexander Weigmann (Managing Director)
Albert Stamate (External Data Protection Officer)
If you have any questions about data protection, please contact: dataprotection@workperfect.de