XING SE Data Protection Committee Annual Report 2018

As the largest online business network in German-speaking countries, we at XING have a major responsibility. With a member base now exceeding the 15 million mark, our members expect us to use and process their data as intended and in a legally compliant manner. We set great store on upholding this trust and guaranteeing maximum privacy and data protection. As a German company based in Hamburg, we have always been subject to strict German data protection law, thus making privacy an integral part of our DNA. In May 2018 the EU GDPR came into effect. This led to a number of changes to the legal framework, so we decided to take use this as an opportunity to provide our users with even more transparency. We worked with the Hamburg Commissioner for Data Protection and Freedom of Information to develop the Privacy at XING website which provides users with information and updates about the privacy measures we have in place to safeguard their data.

In 2018 we also established the Data Protection Committee (DPC), which extends beyond the scope of the law, to examine and review the many topics pertaining to data protection and privacy at XING, including legislation, communication and IT security. The DPC consists of the General Counsel/Vice President Legal and Compliance, the Team Lead Security and Technical Risk Management, the Vice President External Affairs and the Data Protection Officer. Specialists from other departments are also consulted as and when required. An overview of the XING employees who support the DPC is available here.

The DPC convenes once every quarter to discuss the latest privacy issues and then take any action deemed necessary in light of these new circumstances. It also holds additional meetings in the event of any urgent issues. The DPC takes detailed meeting minutes to document its activity and the action it takes. It pledges to provide regular updates by publishing an annual report.

Annual report 2018:

The DPC focussed on the following topics in 2018:

1. Use of browser extensions at XING
2. Review of external service providers’ privacy and security measures and policies
3. Establishment of a Data Protection and Information Security Team

1. Use of browser extensions at XING:

XING employees have access to a wide range of technical equipment, including laptops and smartphones. Employees are entitled to use the equipment that XING issues for both private and professional purposes provided they comply with the XING IT policy. When using such equipment, XING employees may download and install browser extensions (sometimes also known as add-ons). This presents the theoretical risk of XING employees sharing business secrets or other information worthy of protection with browser extension providers or other third parties.

The DPC therefore introduced a series of measures to uphold the principle of maximum data security and minimise the potential risk posed by browser extensions. These measures are reviewed regularly and updated as and when necessary. Technical measures include reviewing relevant extensions and blocking or removing them if they are found to
constitute a security risk. The DPC maintains and regularly updates a whitelist of approved browser extensions which employees can install without any security risk. The DPC also decided to make XING employees (more) aware of the potential risk of installing and using browser extensions so as to prevent data from being passed on to third parties.

2. **Review of external service providers’ privacy and security measures and policies:**

The DPC reviewed two external software solution providers which XING contracts to ensure they have sufficient privacy measures in place. Both providers met the required standards, meaning that XING was able to continue cooperating with them. The DPC revised and tightened the minimum technical requirements that external service providers are required to meet before XING awards service contracts. In addition, the DPC takes steps to ensure that XING employees are regularly made aware of the privacy risks involved in using external software tools and services.

3. **Establishment of a Data Protection and Information Security Team:**

In 2018 the DPC also formed a new team to act as an internal partner with the aim of ensuring that XING has solutions available to meet increasing data protection and privacy requirements as a whole. The newly formed Data Protection and Information Security Team acts independently of the DPC and focuses on the operative implementation of data protection and information security issues, while also being responsible for XING’s Data Protection and Information Security Policy as well as the Data protection guidelines (for employees). The collaboration between the DPC and the Data Protection and Information Security Team ensures that XING is well-versed in all conceptual and practical privacy issues. This means that in spite of increasing requirements, XING has processes in place to ensure it can uphold its pledge to provide members with maximum privacy, data protection and data security.