COSMOS
Navigate the Compliance Universe

CEP Magazine - April 2020
The GDPR is not a shield against internal investigations

By Konstantin von Reden-Lütcken, MBA

Konstantin von Reden-Lütcken (krl@krl-law.de) is a Berlin-based criminal defense lawyer specializing in economic and tax criminal law, forensic investigations, and compliance risk management.

Data protection shifted into focus over the last few years as personal data became more prominent and sensitivity increased in respect to potential misuse. When the General Data Protection Regulation (GDPR)[1] was announced in 2016 to become valid in May 2018, panic-like hysteria emerged, pushed by consultants who sought to conquer a share in the consultancy market for data protection. On a daily basis, the question, "Are you GDPR-ready?" was raised in all kinds of communities. The law created or increased a valid sensitivity toward the handling of personal data, but it can also be used to try and avoid prosecution, internal investigations of misconduct, or even criminal offenses of employees or other personnel.

In internal investigations, large volumes of digital data are being evaluated in order to investigate certain suspicions. During such investigations, digital assets are searched by using personal data to identify communications and documents relating to certain employees under suspicion. How does this affect the rights of those employees under GDPR? I was part of a team that was involved in such an internal investigation, and we were confronted with this question by legal counsel. A data protection specialist analyzed the objections raised by the opposing lawyers. The results brought clarification.

The investigation

I was appointed as external counsel to assist an internal task force that had just started to conduct an investigation to assess the potential misconduct of a managing director, a freelance consultant, and a group of employees who all left the company to join a competitor—all within a time frame of three months. A suspicion had been raised by two whistleblowers who had witnessed questionable actions and had reported them to group counsel and the head of internal audit. After initial interviews with the whistleblowers and limited research of backed up emails by the head of internal audit in conjunction with external lawyers, the suspicion was proven to be based on facts. Therefore, a task force was created, of which I became a part. The intensified investigation that followed was primarily conducted by analyzing archived emails of the former employees and the consultant. The result was that proof of substantial criminal behavior could be established relating to breach of copyright, embezzlement, fraud, and theft of data and documents, as well as a substantial breach of noncompetition stipulations. It was my task to evaluate and summarize the facts, which were then used to file a criminal complaint against the former managing director and the consultant (i.e., the leaders of the "gang"), as well as to file a civil lawsuit claiming roughly €7 million in damages.

During the investigation, the defendants' legal counsel had issued a request based on Article 15 of the GDPR demanding copies of all emails relating to the defendants that had been subject to investigation. After the civil lawsuit had been filed, the request was renewed and incorporated in a counterclaim and objection raised against the analysis of the archived emails and their use as proof in the civil lawsuit. The arguments of the defendants' legal counsel were: (1) the archived emails are personal data; (2) the defendants have a right to receive a copy; and (3) the archived emails may not be analyzed, particularly as they also contain private information, and/or presented as proof in a civil lawsuit. The defendants' counsel intended to use the GDPR and a broad reference to Article 6 of the European Convention on Human Rights to suffocate the prosecution from the start. Legal analysis of the raised objections, however, led to a sobering clarification of the real regulatory intent of the GDPR. The legal findings may in their individuality only be applied in conjunction with German law of civil proceedings and the German Data Protection Act. I, however, believe that the legal principles might be applicable in other jurisdictions as well. After all, the intention of this summary is to reduce the hysteria and fear that has arisen from the implementation of GDPR.