

A&O SHEARMAN

Germany: Immediate dismissal of board member for email forwarding to personal account

04 November 2024

During an investigation, it is not uncommon to discover that an individual has forwarded business emails to their private email address. This ruling from the Higher Regional Court Munich shows the potential implications of doing so.

The Higher Regional Court Munich¹ has approved the immediate dismissal ("*fristlose Kündigung*") of a board member for copying his private email address into business email communications on nine occasions. The respective emails contained sensitive company and personal information, such as employee commission entitlements, inquiries under anti-money laundering laws, salary statements of a former chairman, and internal competence disputes of board members.

GDPR breach due to sensitive content of emails

The court found that forwarding emails to a private account constituted processing of personal data within the meaning of Article 6 of the General Data Protection Regulation (GDPR), which was unlawful because it was neither covered by the consent of the data subjects (Art. 6 para. 1 lit. (a) of the GDPR) nor the legitimate interest of the plaintiff (Art. 6 para. 1 lit. (f) of the GDPR). In particular, the plaintiff's interest in storing the communications in order to be able to protect himself from potential liability towards the defendant company was not considered a legitimate interest since, amongst other things, the plaintiff had a right to review relevant documents, if necessary, even after leaving the company (Sec. 810 of the German Civil Code, *Bürgerliches Gesetzbuch*).

The court held that a breach of the GDPR does not always constitute sufficient grounds for an immediate dismissal. However, the court classified the plaintiff's actions as a serious breach due to the sensitive content of the emails and also the repetitive behavior (nine occasions over a period of approx. two months).

It was irrelevant whether or not the board member had agreed upon the forwarding of emails with the chairman since the board had no authority to exempt its members from mandatory GDPR requirements.

The court also rejected the plaintiff's argument that he would have changed his behavior if he had been warned or informed about the illegality of his actions. The court noted that, a warning ("*Abmahnung*") to a board member is not required before an immediate dismissal.

But no breach of confidentiality obligations

The court rejected the argument that the board member had also breached statutory or contractual confidentiality obligations as the plaintiff had neither disclosed the information to third parties nor made it accessible. In the court's view, the mere storage of business emails on a freemail server was not sufficient to constitute such a breach.

Mitigating and aggravating factors

Relevant mitigating and aggravating factors considered by the court included that the plaintiff:

- Had served as a board member for over eight years without any incidents.
- Had not disclosed the sensitive information to third parties, and the GDPR breach had not resulted in the imposition of a fine against the defendant company.
- Had believed that his actions were legitimate and hence did not act secretly.
- Was almost 64 years old at the time of his dismissal.
- Already had a new employment.

Timing of dismissal

The court emphasized that the knowledge of the supervisory board as a collegial body starts the two-week termination period for immediate dismissal under German law. If there is unreasonable delay in convening the board in order to share knowledge of the breach, eg to delay the two week period starting, it can be assumed that the board was convened with reasonable speed (ie knowledge of the breach will be imputed).

This was important in the present case as one of the supervisory board members was copied into two of the emails where the board member had copied his private address. However, the court denied potential knowledge ("*kennenmüssen*") by this supervisory board member and held that such knowledge cannot be assumed because the emails had been classified as "high priority". So, said the court, the supervisory board member's focus could have been on the content of the emails rather than the particular distribution list – even more so since the private email address was copied between two company email addresses and therefore difficult to spot.

Conclusion

It is not uncommon during an investigation to discover that an individual has sent business emails to their personal account. This court decision will be useful in determining what factors should be taken into account to justify immediate termination, if that is the course the company wishes to pursue. The decision also emphasizes the need to act quickly.

Finally, companies must ensure compliance with any data protection obligations that may arise from such incidents, such as reporting obligations.

¹ Higher Regional Court Munich Munich (OLG München), decision dated 31 July 2024, file reference number 7 U 351/23 e, available at: <https://juris.de/r3/document/NJRE001584839> (as at 28 October 2024).

