Insights, News & Events

EMPLOYEE MONITORING IN GERMANY: BALANCING EMPLOYER OVERSIGHT AND WORKER PRIVACY

Insights
Jan 8, 2026

Employers in Germany face a complex legal landscape when monitoring employees' digital communication, including email, internet, and telephone use. Recent legal developments and longstanding constitutional protections create a delicate balance between an employer's legitimate interest in oversight and employees' privacy rights. For multinational employers with operations in Germany, understanding these rules is critical to avoiding legal pitfalls, including criminal liability and evidentiary exclusions. Here's what you need to know and four practical takeaways.

The Legal Framework

German law recognizes that employers have valid reasons to monitor workplace communications, such as preventing misuse, protecting trade secrets, or investigating misconduct. However, these interests clash with employees' right to "informational self-determination" (derived from Articles 2 and 1 of the German Constitution) and the secrecy of telecommunications (Article 10 of the Constitution).

Despite regulations like the General Data Protection Regulation (GDPR), the Telecommunications-Telemedia Data Protection Act (TTDSG), and the Federal Data Protection Act (BDSG), employee data protection remains fragmented. Section 26 BDSG, which implements Article 88 of the GDPR, leaves significant room for interpretation, particularly regarding whether the secrecy of telecommunications applies when private use of company resources is permitted.

Related People

Mauricio Foeth

Of Counsel

+52 55 48992148/+49 1575 8880464

Service Focus

International

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.

Email Monitoring: What Employers Can and Cannot Do

Private Use Allowed: When employees are permitted to use work email for personal purposes, their messages are protected under the secrecy of telecommunications. Employers cannot routinely access the content of private emails. The protection lasts until the communication process is complete: typically, until the email is fully delivered and no longer stored on the server. Notably:

- Accessing stored emails on a device requires the employee's consent under Sections 9 et seq. BDSG.
- Technical solutions, such as separate folders for private emails or prohibiting private use of work accounts, can help mitigate compliance risks.

Criminal Risks: Unauthorized access to private emails may violate Section 206 of the German Criminal Code (StGB), which prohibits the unauthorized interception of telecommunications. Employers could also face liability under Section 202a StGB for accessing password-protected data without authorization. Additionally, Section 206 (2) No. 2 of the German Criminal Code (StGB) may be relevant if, for example, spam filters or virus scanners used in company systems suppress or delete emails. Also, criminal liability under Section 202a StGB may be considered if the employer accesses password-protected data without authorization. However, this is often ruled out because, in practice, access restrictions are rarely overcome.

Exclusively Business Use: If private use is explicitly prohibited, employers have broader monitoring rights, but not without limits. Section 26(1) BDSG permits spot checks of work-related emails if there is a legitimate reason, such as investigating suspected misconduct. However:

- Covert, continuous surveillance is illegal.
- Comprehensive monitoring is only permissible in cases of concrete suspicion of criminal activity, and even then, it must be time-limited and proportionate.

Evidentiary Consequences: Illegally obtained evidence may be inadmissible in legal proceedings, including disciplinary actions or litigation.

Telephone Monitoring: Strict Limits Apply

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.

Monitoring or recording telephone calls – even for work-related purposes – is generally prohibited if private use is permitted, unless there is reasonable suspicion of serious misconduct and this may affect the employment relationship (e.g., disclosure of trade secrets or harassment through the telephone).

- Call metadata (like call duration and start and end time) can only be processed for billing purposes under the TTDSG, and even then, employee consent is typically required.
- Unauthorized recording or disclosure of calls may violate Sections 201 and 206 StGB, exposing employers to fines or criminal prosecution.

Exclusively Business Use: Even when telephones are restricted to business use, content monitoring remains highly restricted. Employers may only record calls in exceptional circumstances, such as:

- Training purposes (like in call centers), provided it is transparent and not continuous.
- Investigating suspected criminal activity, where documented evidence justifies the intrusion.

Key Consideration: Covert monitoring is almost always illegal and risks evidentiary exclusion in legal disputes.

4 Practical Takeaways for Employers

1. Clarity in Policies

- Employers should implement clear, written policies on the permissible use of company email and telephones.
- If private use is allowed, explicit consent for monitoring should be obtained.

2. Technical Safeguards

- Use separate folders for private emails.
- Implement automated filters to flag potential misuse without accessing private content.
- Restrict monitoring to business-related communications unless criminal activity is suspected.

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.

3. Legal Compliance

- Document all monitoring activities to demonstrate compliance with Section 26 BDSG.
- Avoid continuous or covert surveillance and opt for targeted, transparent checks instead.
- Consult legal counsel before implementing retroactive monitoring, as fines for non-compliance apply.

4. Risk Mitigation

- Train managers on lawful monitoring practices.
- Ensure HR and IT departments collaborate to align technical capabilities with legal requirements.

Conclusion

The monitoring of employee communications in Germany is a balancing act. We will continue to monitor developments related to legal changes in Germany and any new rules or guidelines that affect the workplace. Make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information. If you have questions, contact your Fisher Phillips attorney, the author of this Insight, or any attorney in our International Practice Group.

Copyright © 2026 Fisher Phillips LLP. All Rights Reserved.