Employee Monitoring (Germany)

HOLGER LUTZ AND SIMONE BACH, BAKER MCKENZIE, WITH PRACTICAL LAW DATA PRIVACY ADVISOR

Search the Resource ID numbers in blue on Westlaw for more.

A Practice Note providing guidance on laws and issues related to employee monitoring in Germany. This Note discusses the laws applicable to employee monitoring, legal requirements, and employees' rights to notice, to object to monitoring, and to access their personal data contained in the employer's monitoring records. This Note also addresses limitations on prohibiting and monitoring personal communications sent using an employer's systems, issues when monitoring employee-owned devices, using closed-circuit television (CCTV) monitoring in the workplace, monitoring employees' off-duty conduct, collective bargaining and labor relations considerations, and potential sanctions for illegal employee monitoring.

Employers have many legitimate reasons for monitoring employee activity, for example, to manage workplace productivity, enforce company policies, control quality, protect employees' safety, and secure business assets. No single law regulates employee monitoring in Germany. The EU General Data Protection Regulation (GDPR), federal and state-level data protection laws that protect personal data, and other laws including the Telecommunications Act and the Telemedia Act, apply to employers' monitoring activities.

Applicable laws depend on:

- Whether the employer is a:
  - federal public employer;
  - non-federal public employer; or
  - private employer.
- Whether the employer permits or prohibits employees' personal use of its communications systems.

This Note focuses on laws that apply to federal public and private sector organizations. State-level data protection laws regulate monitoring by non-federal public employers and are outside the scope of this Note.

This Note discusses:

- Applicable laws.
- Legal requirements for monitoring.
- Individuals' rights, including notice, opportunities to object to monitoring, and to access, obtain rectification of, and delete monitoring data.
- Employers' obligations to protect and retain personal data collected for monitoring purposes.
- Prohibiting and monitoring personal use of employer systems.
- Monitoring employee-owned devices.
- Using closed-circuit television (CCTV) monitoring in the workplace.
- Monitoring employees' off-duty conduct.
- Collective bargaining and labor relations considerations.
- Enforcement and sanctions for illegal employee monitoring.

APPLICABLE LAWS

THE EU GENERAL DATA PROTECTION REGULATION (GDPR)

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR), which replaced the EU Data Protection Directive (Directive 95/46/EC) (EU Directive), applies in all EU member states starting May 25, 2018. The GDPR broadly defines personal data to include any information relating to an identified or identifiable natural person (Article 4(1), GDPR). Personal data generally includes information that alone or in combination with other information that an organization has or is likely to have access to directly or indirectly identifies an individual data subject. The GDPR applies to personal data an employer collects through employee monitoring.

Many of the EU's core data protection principles remain the same under the GDPR as they were under the EU Directive. However, the

© 2019 Thomson Reuters. All rights reserved.

GDPR does impose new and additional requirements. In addition, the GDPR permits member states to enact national legislation:

- Adopting more specific rules regarding certain topics, including employee data processing, which may affect the requirements applicable to employee monitoring (Article 88, GDPR).
- Restricting or expanding the scope of the GDPR's requirements.

For an overview of the GDPR's requirements, see Practice Note, Overview of EU General Data Protection Regulation (w-007-9580). For more on the GDPR provisions that permit EU member states to implement national legislation deviating from or supplementing the GDPR, see Practice Note, GDPR Member State Permitted Variations and Requirements Chart (w-012-6272).

FEDERAL DATA PROTECTION ACT

Germany recently enacted the new Federal Data Protection Act (*Bundesdatenschutzgesetz*) (BDSG) which replaced the previous BDSG on May 25, 2018 and aligns German data protection law with the GDPR. The new BDSG varies some of the GDPR's requirements. However, the requirements for processing employee personal data and employee monitoring remain largely the same under the new BDSG as they were under the previous law. Starting May 25, 2018, employers' monitoring activities must comply with the requirements of both the GDPR and the new BDSG, unless another law applies to the specific circumstances (see Other Laws).

For more on handling personal data generally under German law, see Country Q&A, Data protection in Germany: overview (3-502-4080) and the Federal Data Protection Commissioner's (Commissioner) website. For more on the provisions of the new BDSG that vary the GDPR's requirements, see Practice Note, German Implementation of the GDPR (w-011-7515).

OTHER LAWS

Several other laws also protect communications privacy and may affect employers' monitoring activities, including:

- An employer's duty of care towards employees, which requires the employer to protect employees' privacy.
- The German Constitution (Article 10(1)), which protects the privacy of correspondence and telecommunications.
- The German Criminal Code, which punishes for violations of the secrecy of telecommunications.
- The German Telecommunications Act (*Telekommunikationsgesetz*) (TKG) (Section 88), which protects the secrecy of telecommunications.
- The German Telemedia Act (*Telemediengesetz*) (TMG).

German data protection authorities view employers that permit personal use of their communications systems as telecommunication service providers under the TKG or telemedia service providers under the TMG. The TKG generally prohibits telecommunication service providers from monitoring individuals' communications. Similarly, the TMG typically prevents telemedia service providers from processing information about individuals' website access.

The terms of the TMG governing the processing of information about individuals' website access by telemedia service providers are based on the EU Directive which the GDPR replaced (Article 94, GDPR).

This Note discusses the TMG even though it has not yet been officially adapted to the GDPR. The relevant terms of the TKG remain applicable to employee monitoring because they are not based on the EU Directive but instead implement certain provisions of the ePrivacy Directive (Directive 2002/58/EC) (Article 95, GDPR).

If the employer prohibits personal use of its communications systems, the TKG and the TMG do not apply to the employer's monitoring activities. For more on personal use of employer communications systems, see Prohibiting and Monitoring Personal Use of Employer Systems.

DATA PROTECTION AUTHORITY GUIDANCE

Some German data protection authorities have issued guidelines on the use and monitoring of electronic communications systems in the workplace. These guidelines are non-binding but provide useful insight on how German data protection authorities interpret the law. For example, the Conference of independent Federal and State Data Protection Authorities (Conference) issued guidance on the use and monitoring of electronic communications in the workplace in January 2016. This guidance explains the conditions:

- Under which employees are allowed to use the company IT systems for personal purposes.
- Applicable to the employer's monitoring of employees' use.
- Applicable to employers accessing employees' communications.

This guidance is available in German on the data protection authorities' websites.

MONITORING EMPLOYER-OWNED COMMUNICATION SYSTEMS

GDPR Article 88 permits EU member states to adopt more specific rules on employee data processing. Based on GDPR Article 88, Section 26 of the BDSG provides the primary justification for processing employee data for monitoring purposes. The BDSG permits employers to collect, process, and use employee personal data for employment-related purposes where necessary:

- For hiring decisions.
- After hiring for carrying out or terminating the employment contract.

(Section 26, BDSG.)

Employers may only collect, process, and use employee personal data to detect crimes if all the following are true:

- There is a documented reason to believe the employee committed a crime while employed.
- The collection, processing, and use are necessary to investigate the crime.
- The employee's legitimate interests do not outweigh the employer's.
- The type and extent of processing are proportionate to the purpose.

(Section 26(1), BDSG.)

Section 26 of the BDSG does not apply to justify employee monitoring if the monitoring is neither necessary for:

- Purposes of entering into, performing, or terminating the employment contract.
- Investigating a committed crime.

© 2019 Thomson Reuters. All rights reserved.

If Section 26 does not apply the employer may sometimes instead justify the monitoring under Article 6 of the GDPR. GDPR Article 6(1)(f) permits, among other things, data processing necessary to safeguard the employer's legitimate interests, provided the employees' privacy interests do not outweigh the employer's interests. GDPR Article 6(1)(f) does not specifically apply to employee personal data like Section 26 of the BDSG. However, good arguments exist that employers may rely on GDPR Article 6(1)(f) to justify processing employee personal data provided the processing serves the employer's legitimate interests that are only indirectly related to the employment relationship, for example, the prevention of fraud.

Employers should not rely on consent to justify employee monitoring, except in limited circumstances where employees can validly provide consent. For example, when the employer permits personal use of its communication systems and relies on employee consent for certain limited monitoring as a condition of personal use (see Prohibiting and Monitoring Personal Use of Employer Systems).

The BDSG does not expressly permit or prohibit employers from monitoring certain types of employee activities. However, employers should avoid monitoring locations where employees have a reasonable expectation of privacy, for example, changing rooms, restrooms, or other private locations (see Using CCTV Monitoring in the Workplace). Employers must evaluate and justify employee monitoring on a case-by-case basis to ensure compliance with the GDPR, the BDSG and other laws.

If the employer fails to comply with the statutory limitations on employee monitoring, the monitoring is a breach of the data protection law and employers may be prevented from using material from the unlawful monitoring in a later lawsuit. Recently, the Federal Labor Court in Germany (decision 2 AZR 681/16) held that information obtained through use of key logging to monitor an employee's use of the company's internet access and IT systems could not be used to terminate an employee for excessive use of the employer's systems during working time because use of the key logger was unjustified. In particular, the monitoring did not take place to investigate a committed crime of the employee in accordance with Section 32 of the old BDSG and the groundless surveillance was disproportionate. This analysis remains the same under Section 26 of the new BDSG.

CONSENT

German law generally does not require employee consent to monitoring, unless the employer permits personal use of its communications systems (see Prohibiting and Monitoring Personal Use of Employer Systems).

When an employer permits personal use, the employee may either:

- Consent to monitoring and engage in personal use of the employer's systems, subject to the conditions set by the employer.
- Withhold consent and refrain from personal use.

German data protection authorities have questioned the validity of personal data processing based on employee consent. Valid consent must be freely given, and in the employment context, where there is a clear imbalance of power, an employee's consent may not be voluntary. The GDPR imposes specific requirements to obtain valid consent. Consent must comply with GDPR Articles 4(11) (definition of consent), 7 (Conditions for consent) and 6(1)(a), which requires data subjects to give consent for specified purposes. For more on relying on consent in the employment context under the GDPR, see Practice Note, Employee Consent Under the GDPR (w-004-5144).

In addition, if the employer relies on consent to process employee personal data collected through monitoring, whether the employee validly consented depends on:

- The employee's level of dependence in the employment relationship.
- The circumstances under which the data subject consented.

(Section 26(2), BDSG.)

Employers basing monitoring on consent should:

- Properly inform employees about the scope and purposes of monitoring, and the consequences of withholding consent, for example, that the employer does not permit personal use of its communications systems if the employee withholds consent (see Notice).
- Ensure their processes comply with applicable legal requirements for obtaining valid consent.
- Inform employees about their right to revoke consent and its consequences, for example, that the employer does not allow personal use of its communications systems if the employee revokes consent.
- Obtain consent in a form allowing the employer to demonstrate that the employee consented to personal data processing (Article 7(1), GDPR).

INDIVIDUALS' RIGHTS

The GDPR provides employees and non-employees affected by an employer's monitoring activities with several rights, including:

- Prior notice (see Notice and Notice and Consent for Non-Employees).
- Opportunities to object to monitoring under certain circumstances (see Objections to Monitoring).
- Opportunities to restrict the processing of their personal data under certain circumstances (see Processing Restrictions).
- Access to monitoring records and the opportunity to request rectification and deletion (see Records Access, Rectification, and Deletion).

NOTICE

The GDPR grants data subjects, including employees, the right to receive certain information about the employer's personal data collection and processing activities, subject to limited exceptions (Articles 13 and 14, GDPR and Sections 32 and 33, BDSG). These notice requirements apply to employee monitoring.

Employers typically include notice of monitoring in either a:

- Broader employee privacy notice.
- Special notice on monitoring.
- General information technology (IT) policy, such as an IT acceptable use policy.

© 2019 Thomson Reuters. All rights reserved.

Employers may also cover employee monitoring in a works council agreement, if applicable (see Collective Bargaining and Labor Relations).

Employers can generally only use the personal data collected through employee monitoring for the purposes previously notified to the employee, unless they provide a new notice (Articles 13(3) and 14(4), GDPR) (see Data Retention).

Notice Content Requirements

The GDPR requires notices to include the following information:

- The employer's identity and contact details, and if applicable, its EU representative's identity and contact details.
- Contact details for the employer's data protection officer, if applicable.
- The purposes for which the employer processes any personal data collected.
- The legal basis for the processing.
- The categories of personal data the employer collects if it does not collect the personal data directly from the data subject.
- Identification of the data controller's legitimate interests when they serve as the legal basis for data processing.
- The recipients or categories of recipients of the personal data, if any.
- Whether the employer intends to transfer personal data outside of Germany and the data transfer mechanism it uses to legalize the transfer.
- How long the employer stores the personal data or the criteria the employer uses to determine retention periods.
- Whether the employee must provide the personal data by statute, contract, or for another reason, and the consequences of not providing the personal data.
- Whether the data controller uses automated decision-making, including profiling, the auto-decision logic used, and the consequences of this processing for the employee.
- The source of the personal data including whether it came from publicly accessible sources, if it does not collect the personal data directly from the data subject.
- The employee's rights including:
  - rights of access, rectification, erasure, restriction, objection, and data portability;
  - the right to withdraw consent and how to exercise that right if the employer obtains employee consent to justify personal data processing; and
  - the right to make a complaint with a local data protection authority and how to exercise that right, if applicable.

  (Articles 13 and 14, GDPR.)

For more on the GDPR's notice requirements, see Practice Note, Data Subject Rights Under the GDPR: Information Right (w-006-7553).

Notice Exceptions

The GDPR and German law provide limited exceptions from the notice requirements (Articles 13(4) and 14(5), GDPR and Sections 32 and 33, BDSG). The notice requirements do not apply to the extent:

- The monitored employee already has the information (Articles 13(4) and 14(5)(a), GDPR).
- The data controller obtained the information from a source other than the data subject and providing the information:
  - proves impossible or would involve a disproportionate effort; or
  - is likely to render impossible or seriously impair the achievement of the processing objectives. For example, if the employer engages in employee monitoring to investigate a crime, notice may be counterproductive.

  (Article 14(5)(b), GDPR.)

OBJECTIONS TO MONITORING

Employees may object to illegitimate monitoring activities and obtain erasure of unlawfully processed data under GDPR Article 17, but have limited rights to object to legitimate monitoring. An employer is only obligated to stop lawful monitoring if the employer bases the monitoring on GDPR Article 6(1)(e) (processing necessary for a task carried out in the public interest) or 6(1)(f) (processing necessary to pursue the data controller's or a third party's legitimate interests) and the employee objects to the monitoring on grounds relating to his particular situation.

The employer must stop processing the personal data unless:

- The employer demonstrates compelling legitimate grounds for the processing which override the employee's interests, rights, and freedoms.
- The processing is necessary to establish, exercise, or defend legal claims.

(Article 21(1), GDPR.)

Section 36 of the BDSG may limit employees' right to object to monitoring by public employers if there are compelling public interests in the monitoring that outweigh the employees' interests or if applicable law requires the monitoring.

For more on objection rights, see Practice Note, Data Subject Rights Under the GDPR: Data Processing Objection Right (w-006-7553).

NOTICE AND CONSENT FOR NON-EMPLOYEES

Employee monitoring may result in the collection of non-employees' personal data, for example, through telephone recordings, email monitoring, and CCTV use. The GDPR and the BDSG also apply to the collection, processing, and use of non-employees' personal data. Accordingly, the employer must have a valid legal basis for processing non-employees' personal data and must notify non-employees about potential personal data collection. The legal basis that justifies employee monitoring does not automatically justify violating non-employees' privacy rights through monitoring.

To notify non-employees about personal data collection through telephone recordings, organizations should use a pre-recorded telephone message informing non-employee incoming callers and call recipients that (in addition to fulfilling the other information obligations under GDPR Articles 13 and 14):

- The organization may record the telephone conversation.
- The purpose for recording, such as quality control.

© 2019 Thomson Reuters. All rights reserved.

Providing this type of notice does not justify the monitoring and related processing of the non-employees' personal data. Employers must also have a legal basis to justify collecting non-employees' personal data through employee monitoring. Including a pre-recorded telephone message is not sufficient to justify monitoring non-employees.

Employers should also notify non-employees about CCTV use (see Using CCTV Monitoring in the Workplace).

Valid legal bases for collecting non-employees' personal data under the GDPR through employee monitoring include:

- When data processing is necessary to safeguard the employer's legitimate interests and the privacy interests of non-employees do not outweigh the employer's interests (Article 6(1)(f), GDPR).
- When the employer uses CCTV, for example, to pursue its legitimate interests for specifically defined purposes and there is no reason to believe that the privacy interests of non-employees outweigh the employer's interests (Section 4, BDSG). However, due to the priority of the GDPR, BDSG Section 4 only applies where video surveillance takes place in the public interest or in the exercise of official authority vested in the employer (Article 6(1)(e) and 6(3), GDPR).
- When the law does not provide for a legal basis to monitor non-employees but the employer obtains non-employees' consent to monitoring (Article 6(1)(a), GDPR) (see Consent).

Even if the non-employee communicates with the employer or its employees despite knowledge of the monitoring, it is risky for employers to rely on implied consent of the non-employee.

PROCESSING RESTRICTIONS

The GDPR grants employees the right to restrict the processing of their personal data under certain circumstances, including when the employee objects to processing based on the employer's legitimate interests (see Objections to Monitoring) (Article 18, GDPR). For more on the right to restrict data processing, see Practice Note, Data Subject Rights Under the GDPR: Data Processing Restriction Right (w-006-7553).

RECORDS ACCESS, RECTIFICATION, AND DELETION

The GDPR grants individuals the right to access, obtain rectification of, and delete their personal data, including monitoring data, an employer holds about them, subject to limited exceptions (Articles 15, 16, and 17, GDPR). The GDPR also introduces new data subject rights including the right to:

- Restrict data processing under certain circumstances (Article 18, GDPR) (see Processing Restrictions).
- Data portability under certain circumstances (Article 20, GDPR).

The GDPR requires employers to respond to data subject requests within one month, with some opportunities to extend the response time (Article 12(3)). For more on data subjects' rights under the GDPR and data controller obligations see, Practice Note, Data Subject Rights Under the GDPR: Data Subject Rights Under the GDPR (w-006-7553) and Data Controller Obligations Relating to Data Subject Rights (w-006-7553), and Responding to Data Subject Requests Under the GDPR Checklist (w-008-4175).

For information on exceptions to data subjects' rights under the new BDSG, see Practice Note, German Implementation of the GDPR: Data Subjects' Rights.

PROTECTING AND RETAINING PERSONAL DATA

The GDPR requires organizations to:

- Take a risk-based approach to securing personal data.
- Implement technical and organizational security measures appropriate to the risk.

(Article 32, GDPR.)

For more on protecting personal data under German law, see Practice Note, Information Security Considerations: Germany (w-006-6878).

DATA TRANSFERS

Transfers to Third-Party Service Providers

In some situations, an employer may want to share employee monitoring records with third-party service providers inside or outside of Germany or an overseas group company, or an overseas parent may want to conduct the monitoring on behalf of the employer. Employers transferring personal data to service providers (including to other group companies) must:

- Execute a data processing agreement with the service provider containing certain required clauses (Article 28, GDPR).
- Assess the adequacy of the third party's technical and organizational measures prior to the engagement and regularly during the services.
- Ensure adequate protection at the service provider if the service provider is located in a country outside of the European Economic Area (EEA) (Article 44, GDPR). If the service provider is located in a non-European country that has not been recognized by the European Commission as providing an adequate level of data protection, the employer may transfer the personal data, for example, on the basis of:
  - the Standard Contractual Clauses (Controller to Processor) under Commission Decision 2010/87/EU;
  - binding corporate rules (only applicable for group internal data transfers); or
  - the EU-US Privacy Shield framework for transfers from the EU to the US under Commission Decision 2016/1250.

Transfers to Third-Party Data Controllers

If the employer transfers personal data to a third party who is not engaged as a dependent service provider but who receives the data for its own purposes (data controller), the requirement to enter into a data processing agreement does not apply. For transfers to third-party data controllers, the employer must:

- Rely on another legal basis for the disclosure to and independent processing of the personal data by the third party (for example, Article 6, GDPR).
- Ensure adequate protection for data transfers outside of the EEA to recipients in inadequate countries by concluding, for example, the Standard Contractual Clauses applicable to Controller to Controller transfers under Commission Decision 2001/497/EC (Set I), or Decision 2004/915//EC (Set II).

© 2019 Thomson Reuters. All rights reserved.

Employers cannot justify transfers to other (non-European) group companies or the (non-European) parent company (whether it is a data controller to data controller or data controller to data processor transfer) simply because the employer is part of an (international) group structure.

For more information on cross-border data transfers under the GDPR, see Practice Note, Cross-border transfers of personal data under the GDPR (w-013-9203) and GDPR Cross-Border Transfers Checklist (w-011-4081).

DATA RETENTION

German law does not specify a retention period for employee personal data obtained through monitoring. Employers should generally only retain personal data, including monitoring data, for as long as necessary to accomplish the purposes for which they collected it, subject to applicable laws that may require a longer retention period (Articles 5(1)(e) and 17(3), GDPR). Retention periods may vary depending on the monitoring's purpose. Employers should delete monitoring data as soon as they no longer need it for their original purposes, unless they have another legal basis for processing it.

The retention period for monitoring data can often be short. For example, if an employer implements video monitoring to protect its employees and assets, it should dispose of the recordings once it determines that no incidents have occurred. German data protection authorities generally take the position that employers should delete video recordings within 48 hours. Employers may sometimes need to retain monitoring data for longer time periods, such as to resolve a lawsuit or other dispute, or while addressing an incident.

If the employer retains monitoring data for other reasons, for example to satisfy archiving, tax, or accounting requirements, it should avoid processing the personal data for other purposes by blocking the data.

Where video surveillance is subject to Section 4 of the BDSG (see Using CCTV Monitoring in the Workplace), this section further limits employers from using personal data collected through video surveillance for a new or different purpose. The law permits new or different purposes of use only to the extent required to:

- Avert dangers to state security or public safety.
- Prosecute crimes.

(Section 4(3), BDSG.)

PROHIBITING AND MONITORING PERSONAL USE OF EMPLOYER SYSTEMS

The laws and best practices applicable to employee monitoring depend on whether an employer permits or prohibits personal use of their communications systems.

PROHIBITING PERSONAL USE

German law allows employers to prohibit employees' personal use of their communications systems. Employers that prohibit personal use of their communications systems:

- Are unlikely to be subject to the TKG and the TMG.
- Enjoy broader monitoring rights (see Other Laws and Permitting Personal Use).
- Are subject to data protection laws, including the GDPR and BDSG.
- Should enforce the prohibition and impose sanctions for violations.

Failing to enforce prohibitions on personal use may result in application of the TKG and TMG (see Permitting Personal Use).

Employers that prohibit personal use:

- Should use anonymized data to make spot checks to confirm whether employees only use the internet for business purposes.
- May take note of incoming and outgoing business email metadata and ask employees to forward certain emails if required for purposes of the employment relationship or for legitimate business reasons. However, employers may not require employees to auto-forward all emails unless an employee is absent and an out-of-office reply is insufficient.
- Should **not** review personal emails. When employers recognize the personal character of an email, any further processing of the email is generally prohibited.
- Should **not** monitor all email, internet, and telephone use unless the employer is investigating a crime. If, exceptionally, comprehensive monitoring is justified for purposes of investigating a crime, the investigation must be proportionate. For example, when reviewing suspicious emails, it is advisable to do so only in the employee's presence (and possibly in the presence of a member of the works council, if any), as this will be considered less invasive to the employee's privacy than secret monitoring.

PERMITTING PERSONAL USE

Employers that permit or tolerate personal use likely qualify as telecommunication service providers under the TKG and telemedia service providers under the TMG.

The TKG prohibits telecommunication service providers from monitoring individuals' communications. The TMG similarly prevents telemedia service providers from processing information about individuals' website access and browsing history. Employers' rights to monitor employees are significantly restricted if the TKG and TMG apply. Employers can only access data subject to the TKG and TMG secrecy provisions with employee consent or subject to a narrow statutory exception, for example, employers may access this data if required to provide and bill services or to identify or correct defects in the telecommunications equipment.

Employers that permit personal use should:

- Conclude a works council agreement outlining the scope of permitted personal use of their communications systems and the employer's monitoring rights, if there is a works council in place.
- In the absence of a works council, include the scope of permitted personal use and the employer's monitoring rights in individual employment contracts or their IT policy.
- Obtain consent to monitoring from employees (see Consent).

Employers may use spot checks to confirm whether employees adhere to their rules on personal use. Employers should only use anonymized data for these checks unless they have a specific suspicion of misuse.

© 2019 Thomson Reuters. All rights reserved.

MONITORING PERSONAL COMMUNICATIONS

The TKG and the TMG prohibit employers that permit personal use of their communications systems from opening personal emails sent through an employer-owned email address (see Other Laws and Permitting Personal Use). The secrecy of telecommunications provisions under the TKG and the German Constitution:

- Protect not only the communications' content but also the fact that a particular individual was involved in a communication.
- May prohibit an employer that permits personal use of its communications systems from monitoring the employee's business email account, when doing so would result in the employer having knowledge of personal emails.

Employers may not monitor emails sent from a personal, web-based email account even if the employee sends the messages using a business computer or network.

Employers that prohibit personal use of their communications systems have broader rights to monitor employee activities and access the employee's business email account (see Other Laws and Prohibiting Personal Use).

MONITORING EMPLOYEE-OWNED DEVICES

An employer can monitor an employee's use of a personal device when the employee uses the device for business purposes if it:

- Complies with the same requirements applicable to monitoring employer-owned communications systems and devices.
- Implements an agreement with the employee, for example, through a bring your own device to work (BYOD) program, that allows the employer to access and monitor the employee's device.

Employers should implement BYOD programs in a way that balances the organization's information management requirements with employees' privacy expectations. Implementing mobile device management software can:

- Help manage personal devices that connect to the organization's network and systems.
- Partition work-related information and activities from personal activities, and restrict the flow of information between the two.
- Allow the employer to monitor only the work-related activities on the device.
- Give the employer more control over the work portion of the device, including monitoring communications sent and received via a work email account.

Employers should clearly explain the scope of their access and monitoring rights in their BYOD policy or employee agreement.

CONSENT TO MONITOR EMPLOYEE-OWNED DEVICES

Employers must obtain consent to access and monitor the personal devices that employees use for work-related purposes. Employees can validly consent to personal device monitoring in consideration for the employer's permission to use them for business purposes, despite German data protection authorities' view that employee consent may be invalid (see Consent).

Employers cannot require employees to use personal devices for business purposes and consent to monitoring. However, employers can provide employees with the option to use personal devices for work-related matters subject to certain conditions, such as consenting to monitoring and agreeing to follow related policies.

USING CCTV MONITORING IN THE WORKPLACE

USES AND RESTRICTIONS

The BDSG permits video surveillance in publicly accessible areas when necessary, if there are no indications that individuals' legitimate interests outweigh the employer's interests in monitoring, to:

- Fulfill public tasks.
- Exercise the right to determine who shall be allowed or denied access.
- Pursue legitimate interests for precisely defined purposes.

(Section 4, BDSG.)

Due to the priority of the GDPR, BDSG Section 4 only applies where video surveillance takes place in the public interest or in the exercise of official authority vested in the employer (Article 6(1)(e) and 6(3), GDPR).

German law generally does not permit covert surveillance (Section 4, BDSG), except under special circumstances when notice would defeat the monitoring's purpose. For example, covert surveillance can be appropriate when an employer needs to investigate a possible crime and notification would prejudice the success of the investigation. Employers must carefully weigh their interests against employees' and ensure that any monitoring activities are proportional to their purposes, particularly when using covert surveillance.

VIDEO CAMERA LOCATIONS

Employers may not use CCTV surveillance in areas where employees have a reasonable expectation of privacy such as restrooms, changing rooms, and otherwise private areas. Installing cameras in private areas is a violation of the German Criminal Code (Section 201a (1)).

Employers should position cameras to meet their stated purposes of monitoring. For example, to protect facilities against intruders, an employer may decide to install cameras at each entrance and exit, but cameras may not be necessary throughout the facility for this purpose.

NOTICE AND CONSENT FOR CCTV MONITORING

The notice and consent requirements for CCTV use are generally the same as they are for other types of monitoring (see Notice and Consent).

Employers can include the use of CCTV monitoring in a:

- Broader employee privacy notice.
- Special notice on monitoring.
- General IT policy such as an IT acceptable use policy.

If CCTV monitoring occurs in publicly accessible areas, employers must provide a notice of CCTV monitoring clearly indicating the area of surveillance (Section 4, BDSG). The employer must install

© 2019 Thomson Reuters. All rights reserved.

the sign in a place that makes individuals aware of the surveillance at the earliest possible time (except in the limited situations where covert monitoring is permissible). For more information on notice requirements generally, see Notice.

The signs should:

- Contain a clear and understandable notice that the organization uses cameras on the premises and they might capture individuals' images.
- Include the name and contact information of the data controller if individuals have questions or want to access their own images.
- List the contact details of the data protection officer, if any.
- List the purposes of and legal basis for the processing.
- Identify the legitimate interests pursued.
- Include the storage periods or the criteria for determining the storage periods.

CCTV signs should also refer individuals to where the employer provides more detailed information that complies with Articles 13 and 14 of the GDPR.

For more information on providing notice to and obtaining consent from non-employees, see Notice and Consent for Non-Employees.

MONITORING EMPLOYEES' OFF-DUTY CONDUCT

Surveillance of employees' off-duty conduct is subject to the same legal requirements as other types of employee monitoring. Monitoring off-duty conduct involves greater intrusion into employees' private lives so employers should carefully balance their legitimate interests against employees' privacy interests. Employers usually do not have a legitimate reason to monitor off-duty conduct, and employees' privacy interests generally outweigh any interest the employer may have in monitoring off-duty conduct.

However, in exceptional cases, it may be reasonable for employers to monitor employees' off-duty conduct. For example:

- If an employee takes a leave of absence such as a disability leave, and the employer has a reasonable suspicion that the employee is being dishonest. The employer must still carry out the monitoring in a reasonable manner. In exceptional cases, it may be reasonable to take photographs or videos of off-duty employees while they are in public, but not through windows or doors while they are in their homes.
- If an employer provides an employee with a company vehicle, but does not permit personal use, the employer may, in exceptional cases, be able to use GPS tracking to ensure that the employee is not using it outside of work hours.

COLLECTIVE BARGAINING AND LABOR RELATIONS

Works councils have a right of co-determination before employers use any devices or systems to monitor employee activities (Section 87(1) No. 6 Works Constitution Act). Collective bargaining agreements may also govern monitoring where Section 87(1) provides a co-determination right.

The main purpose of the co-determination right is to give employees a voice in certain business decisions. Workers choose individuals to represent them on the works council. The co-determination right applies even if the main purpose of the device or system is not to monitor employees, as long as it has the capability. The right also applies to any change in established monitoring activities.

Individual employment contracts may also address monitoring. For example, an employer may permit personal use of its communications systems if employees agree to monitoring and access by the employer.

ENFORCEMENT AND SANCTIONS

Intentional or negligent violations of data protection obligations are administrative offenses punishable by a fine of up to EUR 20,000,000 (Article 83, GDPR). In addition, the BDSG (as permitted by GDPR Article 84) provides for criminal sanctions for violations of data protection obligations. For example, unjustified processing of personal data not publicly available is a criminal offense punishable by up to two years imprisonment or a monetary fine if committed in exchange for monetary or property gain, to benefit the employer or another party, or with the intent to harm the employee or another individual (Section 42, BDSG).

Violations of the secrecy of communications (see Other Laws) are a criminal offense under the German Criminal Code (Section 206) punishable by imprisonment of up to five years or a monetary fine.

Video surveillance of employees in areas where employees have a reasonable expectation of privacy, such as changing rooms or restrooms, is a criminal offense punishable by imprisonment of up to two years or a monetary fine (Section 201a (1), German Criminal Code) (see Video Camera Locations).

ABOUT PRACTICAL LAW

Practical Law provides legal know-how that gives lawyers a better starting point. Our expert team of attorney editors creates and maintains thousands of up-to-date, practical resources across all major practice areas. We go beyond primary law and traditional legal research to give you the resources needed to practice more efficiently, improve client service and add more value.

If you are not currently a subscriber, we invite you to take a trial of our online services at **legalsolutions.com/practical-law**. For more information or to schedule training, call **1-800-733-2889** or e-mail **referenceattorneys@tr.com.**

02-19

© 2019 Thomson Reuters. All rights reserved. Use of Practical Law websites and services is subject to the Terms of Use (http://static.legalsolutions.thomsonreuters.com/static/agreement/westlaw-additional-terms.pdf) and Privacy Policy (https://a.next.westlaw.com/Privacy).