CEJ
COMPLIANCE
ELLIANCE
JOURNAL

HOW TO CONDUCT E-MAIL REVIEWS IN GERMANY

Practical guidance to avoiding fines, exclusion of evidence and other risks

Tim Wybitul

AUTHOR

Tim Wybitul is a partner of Hogan Lovells and heads the law firm's Compliance & Investigations group in Frankfurt. He helps his clients solving problems regarding data privacy, compliance, internal investigations and labor law requirements. The German Superior Civil Court (Bundesgerichtshof) and the Superior Labor Court (Bundesarbeitsgericht) quote his publications. The German lawyer ranking handbook JUVE and other rankings list him among Germany's leading data privacy and compliance/investigations lawyers.

ABSTRACT

Information from business emails is often very important for investigating breaches of rules or for court proceedings. However, strict legal requirements apply to the analysis and inspection of emails. The following overview sets out these requirements and describes the risks resulting from failure to comply with them, while focusing primarily on more recent court rulings. The article also shows how employers can effectively mitigate or avoid legal risks when monitoring emails. One of the main focuses of the overview is on recommended actions to take in practice and a checklist for preparing for and implementing access to business email accounts.

TABLE OF CONTENTS

I. TYPICAL REASONS FOR ACCESSING BUSINESS EMAILS

In many situations, it may be expedient for companies to access their employees' business email accounts. Nowadays, business transactions are often only documented in emails. It is estimated that emails account for approximately 60–70% of business communication.[1] The growing significance of electronic communication within companies is also increasing the need for appropriate monitoring.[2] A number of common reasons for accessing business email communication are listed below. The focus of the following points – in keeping with their high practical significance – is primarily on monitoring emails for the purpose of internal investigations, preparing for court proceedings or for other measures relating to the investigation of internal company matters.

A. Business interests

For business purposes, it may be advantageous if access to business email accounts is not only available to the individual employee, but also to colleagues or superiors. This not only makes it easier to work together on projects or archive emails, it also enables colleagues to promptly respond to incoming communications if the employee in question is on holiday or off sick.

Companies also have a considerable interest in preventing employees from using their email account to send confidential company data to third parties or to their private email address. Such behavior by employees could fulfill the elements of the offence under sec. 17 of the German Unfair Competition Act [*Gesetz gegen den unlauteren Wettbewerb – UWG*]. In practice, the criminal disclosure of trade and business secrets is often virtually impossible without access to corporate IT systems. Legal responses require that the company in question can also prove such breaches. Any subsequent investigations or criminal proceedings are usually unable to remedy the damage caused by the outflow of data. Employers therefore have a significant economic interest in preventing the illegal outflow of data effectively and in good time before trade secrets are obtained by unauthorized parties. As a rule, this can be achieved by appropriately monitoring email correspondence.

B. Statutory document retention requirements

It may also be necessary to access business email communication in order to meet statu-

---

1 Cf. Frank Peter Schuster, *IT-gestützte interne Ermittlungen in Unternehmen – Strafbarkeitsrisiken nach den §§ 202a, 206 StGB*, 2, ZEITSCHRIFT FÜR INTERNATIONALE STRAFRECHTSDOGMATIK, 68 (2010).

2 Cf. Valerian Jenny, *in* BDSG COMMENTARY GERMAN FEDERAL DATA PROTECTION ACT [BUNDESDATENSCHUTZGESETZ – BDSG], SEC. 88 OF THE GERMAN TELECOMMUNICATIONS ACT [TELEKOMMUNIKATIONSGESETZ – TKG] margin no. 21 *et seq.* (Kai-Uwe Plath et al. eds., 1st ed. 2013).

tory document retention requirements. Electronic business communication may thus be subject to statutory document retention requirements.[3] Emails that are deemed to be commercial letters must be archived pursuant to sec. 238 II *HGB*.[4] If companies wish to meet these obligations, they must also be able to access emails stored on their systems.

C. Requests from German authorities

Furthermore, it is not uncommon for supervisory or prosecution authorities to ask companies to provide emails in order to investigate a particular matter. For example, requests may be made by public prosecutors, the German Federal Cartel Office [*Bundeskartellamt*] or the German Federal Financial Supervisory Authority [*Bundesanstalt für Finanzdienstleistungsaufsicht*]. There are often many reasons for companies to cooperate with the authorities if they receive such requests. However, companies can only provide such assistance in investigating matters if they can access business email communication.

D. Emails as evidence in court proceedings

Electronic communication also plays an important role as evidence in court proceedings.[5] In dismissal protection or damages proceedings, for example, companies can often only prove that employees have breached their duties by presenting the relevant emails. The presentation of internal emails is often requested in cross-border legal disputes, in particular in e-discovery proceedings.[6] For this purpose, too, access rights to employee email accounts are necessary.

E. Detection of breaches of the law, legal duty to conduct investigations

Criminal offences, regulatory offences or other compliance violations can frequently

---

3 E.g. pursuant to sec. 238 II of the German Commercial Code [Handelsgesetzbuch – HGB], sec. 257 I HGB or sec. 147 I of the German Tax Code [Abgabenordnung – AO].

4 Valerian Jenny (*see* footnote 2 above), sec. 88 *TKG* margin no. 21.

5 Cf. e.g. Stefan Sander, *E-Mails und die Beweisführung im Prozess*, 5 COMPUTER UND RECHT (CR) 292 (2014) with further substantiation.

6 Cf. e.g. Axel Spies, *in* Betrieblicher Datenschutz 935 et seq. (Nikolaus Forgó et al eds., 2014); *as well as* Jan Kraayvanger/Mark C. Hilgard, *Urkundenvorlegung im Zivilprozess – Annäherung an das amerikanische „discovery"-Verfahren?*, NEUE JUSTIZ (NJ) 572 (2003); Stefan Hanloser, *e-discovery*, 12 DATENSCHUTZ UND DATENSICHERHEIT (DUD), 785 (2008); Johannes Lux/Tobias Glienke, *US-Discovery versus deutsches Datenschutzrecht*, 9 RIW 603 (2010); Klaus M. Brisch/Philip Laue, *E-Discovery und Datenschutz*, 1 RECHT DER DATENVERARBEITUNG (RDV) 1 (2010); Tim Wybitul, *Interne Ermittlungen auf Aufforderung von US-Behörden – ein Erfahrungsbericht*, 12 BETRIEBS-BERATER (BB) 606 (2009); TIDO PARK, MÜNCHENER ANWALTSHANDBUCH VERTEIDIGUNG IN WIRTSCHAFTS- UND STEUERSTRAFSACHEN, 438 et seq. (Klaus Volk, 2nd ed., 2014).

only be detected or proven by monitoring emails. Secs. 30 and 130 of the German Regulatory Offences Act [*Ordnungswidrigkeitengesetz – OWiG*] set out extensive supervisory duties for companies. These provisions ultimately give rise to a legal duty to conduct internal investigations if there are suspicions pointing to possible breaches of the law. The so-called principle of legality also constitutes a further legal basis of the requirement to investigate matters that point to a breach of the provisions of the German Criminal Code [*Strafgesetzbuch – StGB*] or the *OWiG*. The *District Court* [*Landgericht – LG*] *of Munich I* only recently confirmed in a high-profile judgment that members of the management board must, as part of their legality duty, ensure that the company is organised and supervised in such a way that no breaches of the law occur[7]. Companies only meet these supervisory requirements if they can also carry out monitoring of business email communication in the case of appropriate indications.

II. LEGAL REQUIREMENTS FOR THE INSPECTION OF EMAILS

Substantial legal requirements apply to the analysis or monitoring of business email accounts.[8] In all cases, companies must comply with the strict requirements of the *BDSG*. As a rule, the proportionality principle that must be safeguarded in this respect requires a comprehensive weighing up of the interests of the employees affected by the monitoring of emails against the purpose of the monitoring pursued by the company.[9] The economic interests of the company on the one hand, and the general right to privacy of the persons affected by the inspection or analysis of their emails on the other, must be weighed against each other.

As there are not yet any court rulings setting out clear and generally valid requirements for the inspection and analysis of email accounts, monitoring emails often entails significant legal risks. If mistakes are made in the legal assessment of the permissibility of mon-

7 *So-called* "Neubürger decision", District Court of Munich I, NZG 2014, 345 (not *res judicata*; appeal filed with the Munich Court of Appeals [Oberlandesgericht – OLG] pending under 7 U 113/14); cf. *also* Spieß, CCZ 2014, 143; Meyer, DB 2014, 1063; Holger Fleischer, *Aktienrechtliche Compliance-Pflichten im Praxistest: Das Siemens/Neubürger-Urteil des LG München*, NEUE ZEITSCHRIFT FÜR GESELLSCHAFTSRECHT (NZG) 321 (2014).

8 Cf. e.g. Markus Rübenstahl & Stefanie Debus, *Strafbarkeit verdachtsabhängiger E-Mail- und EDV-Kontrollen bei Internal Investigations*, NEUE ZEITSCHRIFT FÜR WIRTSCHAFTS-, STEUER- UND UNTERNEHMENSSTRAFRECHT (NZWiSt) 69 (2012), *or* Tim Wybitul, *Neue Spielregeln bei E-Mail-Kontrollen durch den Arbeitgeber*, ZEITSCHRIFT FÜR DATENSCHUTZ (ZD) 69 (2011).

9 Cf. Martin Kock & Julia Franke, *Mitarbeiterkontrolle durch systematischen Datenabgleich zur Korruptionsbekämpfung*, NEUE ZEITSCHRIFT FÜR ARBEITSRECHT (NZA) 646, 648 (2009); Wybitul *in* Knierim/Rübenstahl/Tsambikakis, *Internal Investigations*, 2013, 294.

itoring measures, employers face risks of criminal liability,[10] fines,[11] prohibitions on using evidence with regard to the information collected,[12] claims for damages asserted by persons affected by the inspection of their emails, massive reputational damage due to negative reporting in the media and a number of other disadvantages.

A. Monitoring business emails if private use is prohibited

From a legal perspective, it can only be advised that companies prohibit the private use of business email accounts.[13] This is because the permissibility and limits of email monitoring depend heavily on whether the employer allows the private use of the corporate IT system. If the employer prohibits its employees from the private use of business email accounts, it has extremely extensive options with regard to monitoring and supervision. It can then, as a rule, access electronic communication in the company. If private use is prohibited, emails on company servers are treated similarly to business letters.[14] In this case, access to email accounts is governed by the general requirements of data protection, e.g. in the form of sec. 32 I 1 or 2 *BDSG*.[15] Ultimately, the employer must weigh up its own interest in monitoring emails against the right of those affected to informational self-determination.[16]

B. General prohibition on monitoring emails if private use is permitted?

As managing a comprehensive prohibition on private use is not possible in practice, most companies in Germany permit their employees to send and receive private emails via their business account.[17] This approach leads to considerable problems that are described in detail below.

---

10 E.g. pursuant to sec. 44 BDSG or pursuant to sec. 206 I StGB (disputed), cf. also sec. 202 a StGB.

11 In particular pursuant to sec. 43 II no. 1 BDSG.

12 Cf. e.g. BAG, NZA 2014, 143; ZD 2014, 260; *or* Stefan Brink/Tim Wybitul, *Der "neue Datenschutz" des BAG*, ZD 225 (2014) on the inadmissibility of evidence obtained in breach of data protection regulations in civil proceedings.

13 E.g. *also* Riesenhuber, *§ 32, in* Beck Online Kommentar BDSG margin no. 146 (Heinrich Amadeus Wolff et al eds., 4th ed. 2013).

14 Cf. e.g. GREGOR THÜSING, BESCHÄFTIGTENDATENSCHUTZ UND COMPLIANCE margin no. 48 et seq. (2nd ed., 2014); Katrin Stamer & Michael Kuhnke *in* Plath (footnote 2 above), § 32 margin no. 78.

15 *Likewise* Stamer/Kuhnke *in* Plath (footnote 2 above), § 32 margin no. 81.

16 Cf. Regional Labour Court [Landesarbeitsgericht – LAG] of Hamm, judgment of 10 July 2012 – 14 Sa 1711/10, BeckRS 2012, 71605; CCZ 2013, 115 with comments *by* Heinemeyer, CCZ 2013, 116.

17 E.g. also Stamer/Kuhnke, *in* Plath (footnote 2 above), § 32 margin no. 79 *or* Martin Munz, *sec. 88 TKG,* Kommentar zum BDSG margin no. 21 (Jürgen Taeger & Detlev Gabel, 2nd ed. 2013).

a) If private use is permitted, are employers subject to telecommunications secrecy? If private use is not explicitly prohibited, the question arises of whether the employer is a "provider of telecommunications services". The majority of the specialist literature to date views employers as providers of telecommunications services if they permit the private use of corporate email systems.[18] As a result, telecommunications secrecy should also apply to the relationship between the employer and the employee in the case of business emails. Supporters of this view refer to the fact that telecommunications secrecy protects not only the content of a communication conducted by email, but also the detailed circumstances of the telecommunication process.[19] The employer is, therefore, not allowed to access the emails of its employees that are stored on company servers. Otherwise, it breaches sec. 88 *TKG* and possibly also sec. 206 I *StGB*.[20] Furthermore, the majority of the data protection supervisory authorities of the German federal states and the German federal government take this view.[21]

According to this view in the specialist literature, the employer should therefore be barred from accessing *all* email correspondence of the employee.[22] This is because, in order to distinguish between private and business emails, the employer must monitor individual emails and thereby commit a breach of telecommunications secrecy, which is subject to a penalty.[23] This view presents excessive hurdles for companies and is heavily criticised in some cases due to its practical consequences.[24]

---

18 Cf. e.g. Achim Seifert, *§ 32, in* BDSG margin no. 90 (Spiros Simitis, 8th ed. 2014); Peter Gola/Christoph Klug/Barbara Körffer, *§ 32, in* BDSG margin no. 18 (Peter Gola & Rudolf Schomerus, 11th ed. 2012); Ines M. Hassemer, *Strafrechtliche Folgen des Verstoßes gegen Beschäftigtendatenschutz*, *in* Daten- und Persönlichkeitsschutz im Arbeitsverhältnis 549, 571 margin no. 91 (Stephan Weth et al eds., 2014); Theodor Lenckner & Jörg Eisele, *§ 206, in* StGB Kommentar margin no. 8 (Adolf Schönke & Horst Schröder, 28th ed. 2010); Peter Gola, *Neuer Tele-Datenschutz für Arbeitnehmer? Die Anwendung von TKG und TDDSG im Arbeitsverhältnis*, MULTIMEDIA UND RECHT (MMR) 322 (1999); Mengel, Kontrolle der Telekommunikation am Arbeitsplatz, BETRIEBS-BERATER (BB) 1445, 1449 *et seq.* (2004); Christian Oberwetter, *Arbeitnehmerrechte bei Lidl, Aldi und Co.*, NZA 609, 610 et seq. (2008); René Hoppe & Frank Braun, *Arbeitnehmer-E-Mails: Vertrauen ist gut – Kontrolle ist schlecht*, MMR 80 (2010); *ultimately similar* Munz *in* Taeger/Gabel (footnote 17 above), § 88 *TKG* margin no. 23; BeckOK *BDSG*/Riesenhuber (footnote 13 above), § 32 margin no. 144; Stamer/Kuhnke *in* Plath (footnote 2 above), § 32 margin no. 78 et seq.

19 Sec. 88 I 2 *TKG*.

20 Cf. e.g. Martin Munz (*see* footnote 17 above), sec. 88 *TKG* margin no. 20.

21 Cf. Martin Munz (*see* footnote 17 above), sec. 88 *TKG* margin no. 42.

22 E.g. Achim Seifert (*see* footnote 18 above), § 32 margin no. 92.

23 Ulrich Riesenhuber (*see* footnote 13 above), § 32 margin no. 148 describes this view, which is based on the mixing of business and private email communication, as a "scrambled egg theory". Cf. *also* Martin Munz (*see* footnote 17 above), sec. 88 *TKG* margin no. 20.

24 Cf. e.g. Ulrich Baumgartner, 363, 380, *in* Daten- und Persönlichkeitsschutz im Arbeitsverhältnis (Stephan Weth et al eds., 2012)

b) Opposing view: Employers must adhere to the requirements of the BDSG. In the more recent specialist literature, the view is frequently expressed that employers are not telecommunications providers even if they allow their employees private use of business email accounts.[25] There are better arguments in favour of this view than for a rigid application of telecommunications secrecy and a resulting absolute prohibition on monitoring.[26]

The currently prevailing view in the literature regards employers as telecommunications service providers, in particular due to the highly indeterminate wording of sec. 3 *TKG*.[27] However, one of the arguments against this interpretation is that unclearly formulated provisions must initially be interpreted in a manner that is consistent with the constitution. With regard to the question of the permissibility of accessing emails on company servers, the opposing interests of the employer [28] and the employee[29] can only be reconciled in a manner that is consistent with fundamental rights by way of practical concordance.[30] However, this can only be done by weighing up the interests concerned and not on the basis of a strict prohibition on access as stipulated by telecommunications secrecy.

Even if telecommunications secrecy does not apply, the right of users of business email accounts to informational self-determination is protected comprehensively by the *BDSG* as well as the review of proportionality to be conducted pursuant thereto.[31] Access to business email accounts is governed in particular by the data protection provisions under sec. 32 I 1 or sentence 2 *BDSG*.

C. Practical significance of the possible applicability of telecommunications secrecy

The dispute about the question of the scope of application of sec. 88 *TKG* is extremely important for companies. The decisive factor in this respect is what legal consequences could arise from accessing an employee's business emails. Ultimately, it is therefore a

25 Cf. in respect of this conflict of opinions Gregor Thüsing (*see* footnote 14 above), margin no. 74 et seq.

26 Cf. e.g. Gregor Thüsing (*see* footnote 14 above), margin no. 74 et seq.; Ulrich Baumgartner, *in* (*see* footnote 18 above), 363, 380; Tim Wybitul, *Neue Spielregeln bei E-Mail-Kontrollen durch den Arbeitgeber*, ZEITSCHRIFT FÜR DATENSCHUTZ, 69 (2011).

27 Within the meaning of sec. 3 no. 6 *TKG*.

28 E.g. art. 2 I, art. 12 I, art. 14 I of the German Basic Law [Grundgesetz – GG].

29 E.g. art. 2 I in conjunction with art. 1 I GG, art. 10 I GG.

30 As rightly stated *by* Gregor Thüsing (*see* footnote 14 above), margin no. 91.

31 As ultimately also stated in Ulrich Riesenhuber (*see* footnote 13 above), sec. 32 margin no. 146 on prohibited private use.

matter of assessing the legal consequences or of analysing the possible consequences of accessing electronic communication in a company. To do so, it is not only important to be familiar with the legal opinions outlined above. Rather, above all the decisive factor for practitioners is how courts assess the question of the possible applicability of telecommunications secrecy.

D. Requirements laid down by court rulings on monitoring emails if private use is permitted

To date, there have been no rulings of the highest court instances on the question of whether employers that permit private email use are subject to telecommunications secrecy.[32] However, in 2010 the *Regional Labor Court of Lower Saxony*[33] and in 2011 the *Regional Labor Court of Berlin-Brandenburg*[34] addressed the question of whether such employers must be treated as telecommunications providers. The result of both decisions is clear: the judges did not deem the employers concerned to be providers of telecommunications services. Consequently, employers must not take into account telecommunications secrecy in the case of their employees' business emails.[35] The more recent judgments of German courts outlined below are also along these lines.

a) Regional Labor Court of Hamm. Helpful guidance is contained in the judgment of the *Regional Labor Court of Hamm* of 10 July 2012,[36] which concerns the permissibility of the use of chat records in dismissal protection proceedings. In the case of dismissal due to serious breaches of duty, the court granted the employer very extensive options for monitoring the electronic resources provided. In contrast to the private use of business email accounts, there are a number of reasons in favor of the applicability of telecommunications secrecy with regard to the use of chat providers on a workstation. The judges ultimately left open whether the employer must be regarded as a "service provider" within the meaning of the *TKG* in respect of chatting on the workstation. Nevertheless, they granted the company highly extensive monitoring options because the company had previously stated in corresponding guidelines that employees must not expect any confidentiality when using the corporate IT systems:

This can also be applied to accessing business email communication. In its decision, the *Regional Labor Court of Hamm* expressly found that the treatment of chat records

---

32 As also stated *by* Martin Munz (*see* footnote 17 above), sec. 8 *TKG* margin no. 20.

33 Regional Labor Court of Lower Saxony, NZA-RR 2010, 406.

34 Regional Labor Court of Berlin-Brandenburg, NZA-RR 2011, 342.

35 Cf. Ulrich Fülbier & Andreas Splittgerber, *Keine (Fernmelde-) Geheimnisse vor dem Arbeitgeber?*, NEUE JURISTISCHE WOCHENSCHRIFT, 1995 (2012).

36 Regional Labor Court of Hamm, judgment of 10 July 2012 – 14 Sa 1711/10, BeckRS 2012, 71605.

must, as a rule, follow the legal treatment of emails.[37]

The fact that the *Regional Labor Court of Hamm* found in favor of the employer in its weighing up of interests, above all due to the corresponding guidelines, underlines that employers are well advised to retain extensive control and monitoring rights with regard to the IT infrastructure provided. An ever growing number of employers are responding to the more recent court rulings by revising their policy on the use of the Internet and email systems in the company. In this respect, companies should specifically state what use of corporate email systems is permitted and what is not. If the employer wants to ensure that emails can be used in subsequent court proceedings, it should primarily inform its employees of what monitoring measures they must expect and under what circumstances emails will be monitored by issuing corresponding guidelines. This is because the German Federal Labor Court [*Bundesarbeitsgericht – BAG*] is increasingly adopting the approach of not using evidence that has been collected behind the backs of employees.[38] Against this background, employers can only be advised to create a high degree of transparency.

b) Administrative Court [Verwaltungsgericht – VG] of Karlsruhe. The *Administrative Court of Karlsruhe* also expresses a clear view on the question of whether employers that permit the private use of business email accounts must be regarded as service providers within the meaning of the *TKG*:[39]

"The plaintiff invokes the provision under sec. 88 *TKG* entitled "telecommunications secrecy". Pursuant to sec. 88 I 1 *TKG*, telecommunications secrecy applies to the content of the telecommunication and its detailed circumstances, in particular whether someone is or was involved in a telecommunications process. Pursuant to sec. 88 II 1 *TKG*, every service provider is obliged to safeguard telecommunications secrecy. (...)

Even if private use is assumed to be permitted, the legislative purpose of the *TKG* prevents any use of sec. 88 *TKG*. Sec. 1 TKG indicates that the Act aims to promote private competition in the area of telecommunication, therefore that it is geared towards the legal relationships between the state and telecommunications providers as well as those between telecommunications providers. However, the spirit and purpose of the Act is not to govern internal legal relationships – e.g. between employer and employee – within companies or authorities."[40]

---

37 Regional Labor Court of Hamm, judgment of 10 July 2012 – 14 Sa 1711/10, BeckRS 2012, 71605 margin no. 179.

38 E.g. German Federal Labor Court, NZA 2014, 143; ZD 2014, 260 or NJW 2014, 810.

39 Administrative Court of Karlsruhe, NVwZ-RR 2013, 797 margin no. 65.

40 Emphasis by the author.

The *Administrative Court of Karlsruhe* thus arrives at the same conclusion as the *Regional Labor Court of Lower Saxony* and the *Regional Labor Court of Berlin-Brandenburg*. Here, too, the judges correctly reject any applicability of telecommunications secrecy in the employment relationship.

Furthermore, the decision clearly shows that, even without telecommunications secrecy, the right to privacy of those affected by the analysis of their data is protected quite effectively because the administrative judges essentially found in favor of the plaintiff to the extent that his personal data was not permitted to be used any further. They justified this conclusion on the basis of the data protection provisions applicable to the case decided on.[41]

c) Regional Labor Court of Hesse. The *Regional Labor Court of Hesse*[42], too, assesses in a similar manner the question of whether employers are providers of telecommunications services. The case in question related to the summary dismissal of an account manager for deleting business emails, customer contacts and customer appointments of the employer. In the dismissal protection proceedings, the employee submitted that he

"was able to freely dispose of his Outlook account and also used it to save and send private data. (...). Any knowledge regarding the plaintiff's behavior with respect to this data should not be used in the collection of evidence as this violates the plaintiff's general right to privacy."

This line of argument pursued by the plaintiff is consistent with the view outlined above that the employer is not permitted to access emails on company servers if it allows or tolerates the private use of email accounts.

The employer took a different view. After corresponding suspicions had arisen, it asked an expert to prepare an expert opinion in order to establish whether and which emails and other data had been deleted by the account manager. If the *Regional Labor Court of Hesse* had actually deemed the employer's actions as a violation of telecommunications secrecy due to the allegedly permitted private use of the email account, it would not have been allowed to use the expert opinion in the subsequent court proceedings. However, the *Regional Labor Court of Hesse* did not deem that it was prevented from using the expert opinion. Ultimately, the judges thus clearly rejected the restrictive view in the specialist literature. In the grounds for the judgment, the judges stated in this respect:

---

41 In particular on the basis of sec. 15 IV of the State Data Protection Act of Baden-Württemberg [Landesdatenschutzgesetz Baden-Württemberg – DSG BW].

42 Regional Labor Court of Hesse, judgment of 5 August 2013 – 7 Sa 1060/10, BeckRS 2013, 75084; ZD 2014, 377 with comments *by* Thorsten Sörup, *Außerordentliche Kündigung - Datenlöschung - Urlaubsanspruch - unzulässige Verweisung auf einzelne Tarifbestimmungen*, ZEITSCHRIFT FÜR DATENSCHUTZ, 378 (2014).

"Nor is the court prevented from using the result of the taking of evidence determined by the expert opinion, although the analysis of the hard drive submitted to the expert revealed that private emails and private contact addresses were also among the files deleted by the plaintiff.

Given that the computer was provided to the plaintiff as a work tool and the plaintiff used it to process and store a considerable volume of data that he required to perform his duties under his employment contract, the fact that private files of the plaintiff also became known by name during the taking of evidence constitutes such a minor intrusion into his privacy that this does not lead to a prohibition on the use of evidence, and therefore the question of whether the plaintiff was at all permitted to use the defendant's computer for private purposes does not need to be addressed any further."

If the *Regional Labor Court of Hesse* had assumed the possible applicability of telecommunications secrecy in the case described, it would have had to justify why it used the data in question despite the employer violating sec. 88 *TKG* and possibly also sec. 206 I *StGB*. Instead, the judges even clarify in the cited decision that telecommunications secrecy or other restrictions on data use by employers are not applicable in the core area of the employment relationship – regardless of the question of whether the company allows the private use of corporate IT systems.

E. Consequences for companies

As a result, it can be stated that, according to the correct view, telecommunications secrecy does not prevent business email communication from being monitored and analyzed. In fact, employers must adhere to the strict requirements of data protection law. The employer can take into account the general right to privacy of the employee concerned by informing its employees of the possible monitoring of email inboxes (e.g. in a works agreement or IT guidelines) and precisely specifying the conditions for monitoring. Furthermore, employers should only permit the private use of email accounts if employees have consented to any monitoring.

III. CHECKLIST: DATA PROTECTION IN THE CASE OF EMAIL ANALYSIS

The following checklist provides guidance on how to analyze and inspect business emails in accordance with data protection provisions. It does not replace the respective review of data protection requirements in the individual case. In cases of doubt, the company must always perform a review of permissibility based on the circumstances of the respective inspection of emails and the content of the communication concerned.

A. Preparation for the analysis

Companies should always carefully prepare for the monitoring of emails and establish in good time conditions that enable the electronic communication required to realize the specifically pursued purpose of the monitoring to be inspected in accordance with data protection provisions.

a) Review and, if necessary, amendment of existing IT rules. Corporate rules on email use often have a huge influence on the permissibility of analyzing email accounts. As already stated, more detailed monitoring is possible in principle if the employer has prohibited the private use of business email accounts or the users concerned have consented to monitoring. The decisive factor here is whether users are entitled to legitimately expect that email communication is not monitored. In such cases, only restricted access to electronic communication is usually allowed. The corresponding corporate rules on email use can thus have a major effect on the review of proportionality that is necessary for the specific analysis.

b) Composition of the investigation team. The group of persons with access to personal data for the purpose of analyzing emails should be restricted to the minimum needed to effectively investigate the matter. The company should clearly define duties and areas of responsibility. The "need to know" principle applies.

c) Training the investigation team. Extensive knowledge of data protection law is required in order to inspect emails in compliance with data protection provisions. Otherwise, there is, among other things, the risk of criminal liability and fines, of the information and evidence obtained being unusable and considerable reputational damage. Therefore, all members of the investigation team should be trained in the key data protection requirements.

d) Obligation to maintain data secrecy. All parties involved in the inspection must be comprehensively obliged to maintain data secrecy pursuant to sec. 5 *BDSG* and informed of the possible consequences of data protection violations. In particular, the company should also provide information on the risks of fines and criminal liability pursuant to secs. 43, 44 *BDSG* as well as secs. 201 *et seq*. *StGB*.

e) Involvement of data protection experts. As far as possible, an experienced data protection expert should attend each email inspection in order to address questions relating to the individual case. In all cases, this expert must be highly familiar with the aforementioned relevant court rulings on email inspections and on employee data protection.

f) Involvement of the data protection officer. The company's data protection officer should be involved in each phase of the email inspection. If possible, the data protection officer should perform a prior check of the specifically planned measures before the email inspection.

g) If necessary, take into account co-determination rights of the works council. As a rule, the works council has a co-determination right in respect of email inspections pursuant to sec. 87 I no. 6 of the German Works Constitution Act [*Betriebsverfassungsgesetz – BetrVG*]. If the employer disregards this co-determination right, the works council may very quickly obtain a cease and desist order preventing the email inspection from being carried out any further. In addition, sec. 80 I no. 1 *BetrVG* affords the works council extensive information rights with regard to data protection issues. In practice, the conclusion of corresponding works agreements has proven itself as a suitable way to create legal certainty.[43]

h) IT infrastructures. Technical requirements, in particular relating to documentation as well as to data backup and data analysis, are also important. There is a wide range of software solutions for inspecting emails.[44] Corresponding contractual agreements must be concluded with the providers of forensic software and services. In this respect, it must also be examined whether these provisions can be structured as commissioned data processing contracts within the meaning of sec. 11 *BDSG*. At the same time, the company should also carefully check whether the respective contracts offered by the providers meet the relevant legal requirements, cf. in particular sec. 11 II–V *BDSG*.

i) Data security. Pursuant to sec. 9 *BDSG*, a high degree of data security is stipulated in the case of email analysis in particular. This applies especially to entry, access and disclosure controls. It is imperative that these controls guarantee that information from the email inspection does not become known to any unauthorized parties. In particular, the use of USB sticks and other mobile data carriers must be effectively prohibited.

B. Legal framework

In view of the strict requirements for the lawful monitoring of internal electronic communication and the possible serious consequences of data protection errors, companies should carefully ensure that they also implement the measures specified below in order to create a sufficient legal framework.

a) General permissibility of the planned email inspection. Are there reliable statements on the general permissibility of the intended inspection of electronic communication? These could be, in particular, statements by the supervisory authorities for data protection as well as legal expert opinions by data protection experts.

43 Cf. *BAG*, NZA 2014, 551.

44 E.g. Concordance, CT Summation, Kroll Ontrak, Forensic Toolkit.

b) Possible involvement of the data protection authority. One of the safest ways to reliably rule out subsequent legal risks is to liaise with the competent supervisory authority for data protection. If the timeframe of an investigation permits this course of action, companies should certainly examine whether liaising with the data protection authority is possible and expedient in the specific individual case.

c) Data backup. The persons involved in the analysis should only inspect data that is saved in *forensic backup copies*. Intrusion into ongoing email correspondence must be avoided as a matter of urgency. In particular, it should be ensured that, in the course of the inspection of emails, no changes are made to metadata on the company's email servers. Otherwise, the subsequent evidentiary value of the inspected emails could be significantly reduced.

d) Instructions for the investigation team. The persons involved in the analysis should not read emails that are obviously private or stop inspecting private correspondence if they have already started to do so.

e) Informing the persons affected. The persons affected by the inspection of their business email correspondence should be informed as early as possible of the analysis of their electronic communication. In particular with regard to email inspections, German data protection law requires a high degree of *transparency* when handling personal data (sec. 4 II and III as well as secs. 33 *et seq*. *BDSG*).[45] It is often possible to inform the persons affected of the intended inspection of their emails after the mirroring of emails in order to create a forensic backup copy. The situation is different if there are specific indications that, otherwise, the objective of the investigation could be endangered, e.g. by wiping away traces.

C. Implementation of the email inspection

The actual inspection of the electronic communication that is decisive in order to realize the respective purpose of the monitoring is also subject to substantial requirements under data protection law.

a) Confidentiality. Any internal disclosure of the results of an email inspection should be restricted to the absolute minimum required. Any prejudgment or stigmatization of the persons affected by the investigation of the matter must be avoided.

b) Narrowing down the group of persons affected. The group of persons affected by the analysis of their emails must be strictly limited to those required to realize the objective

45 Cf. *BAG*, NZA 2014, 143.

of the monitoring. If a user has no connection to the purpose being pursued by the inspection of the emails, his business email account should not be accessed.

c) Narrowing down the email inspection. The email inspection should be strictly limited to the communication that is relevant for the matter in question, e.g. by being narrowed down to specific periods, business transactions, questionable payments, contractual relationships or agreements, business partners, other persons involved.

d) Weighing up of interests in the individual case. When examining the matter from the perspective of data protection law, it is necessary to weigh up the specific interest of the company in conducting an investigation and the right of the persons affected by the inspection of their emails to the protection of their informational self-determination. If the protection-worthy interest of the person affected by the inspection of his data in the preclusion of the analysis of his emails outweighs the other factors, the inspection *must not be carried out*.

When weighing up these interests – the realization of the objective of the investigation versus the right of the persons affected to informational self-determination – all the circumstances of the respective case and of the individual email communication must be taken into account. As a rule, this *review of proportionality in the individual case*[46] requires considerable prior knowledge of data protection law.

In particular, the respective reader of the email must assess whether the inspection of this specific electronic communication is at all *suitable* for investigating the matter in question, whether there are *milder means* of realizing the objective of the investigation just as effectively and whether the inspection is *reasonable*, i.e. can be conducted on the basis of an appropriate weighing up of the interests of the persons affected and those of the company.

If the inspection of an email is clearly unable to realize the objective of the investigation, it is not *suitable* and therefore not permissible. For this reason, emails that are obviously of an exclusively private nature may not be inspected, for example. Furthermore, the inspection of the emails in question must always be the *mildest of all equally effective means* that are available in order to investigate the matter. This requirement must be ensured in every phase of the investigation of the matter. In particular, according to the court rulings, the highest possible degree of transparency vis-à-vis the employees affected by the analysis of their emails must be ensured.

---

46 Cf. *in detail* in respect of the three-stage review standard Oliver Zöll (*see* footnote 17 above), sec. 32 BDSG margin no. 18; Tim Wybitul, *Wie viel Arbeitnehmerdatenschutz ist "erforderlich"?*, BETRIEBSBERATER, 1085 (2010); TIM WYBITUL, HDB DATENSCHUTZ IM UNTERNEHMEN 175 et seq. (2nd ed., 2014).

Even if the inspection of an email is suitable for realizing the purpose of the investigation or monitoring and constitutes the mildest of all equally effective means, this handling of personal data must always be proportionate in the narrower sense. An email inspection is *appropriate* if legitimate interests of the persons involved in the electronic communication do not outweigh the company's interest in conducting the investigation. In particular, any email inspection that concerns the core area of the affected persons' private lives, e.g. emails of an intimate nature, is prohibited.

e) Review of emails that are problematic from the perspective of data protection law. In practice, it has proved worthwhile for the person involved in the analysis to designate emails that he deems to be problematic from the perspective of data protection law. These emails should only be inspected later after a detailed review of the permissibility of the analysis under data protection law – or if other suspicions indicate that precisely the email communication in question is decisive for the specific purpose of the investigation or monitoring. The assessment of individual emails under data protection law often also changes in the course of the respective investigation because the investigators obtain further information.

f) Graduated approach. As far as possible, the actual inspection should initially focus on random samples instead of a uniform and complete check. Equally, analyses must always relate strictly to the respective objective of the investigation.

D. Documentation of the email inspection

Compliance with the above points should be *documented comprehensively* for evidentiary reasons and in order to avoid considerable disadvantages (up to and including risks of criminal liability). In particular, the points below should be clearly recorded.
As a rule, such documentation is not prepared in writing, but in electronic form. Commercial software solutions that help companies inspect emails usually have corresponding functions for preparing records of email inspections.

a) Specific purposes of the email inspection. Above all, the company should very clearly set out the purposes being pursued by the respective email inspection. This can make it much easier for the company's data protection officer to review the permissibility of the planned measures.

b) Description of the individual steps in the investigation. The company should systematically and clearly determine the individual phases of the respective measures designed to investigate the matter.

c) Search criteria used. The company should record the parameters used to select the electronic communication actually inspected.

d) Email accounts affected. Which accounts were inspected, which periods were affected

by the monitoring of emails?

e) Emails discovered that are relevant to the matter. Finally, the company should document which emails it deems relevant for the matter in question. In addition, it should also record the conclusions to be drawn from these emails for the further investigation of the matter.

IV. SUMMARY AND RECOMMENDED ACTIONS

Complex requirements apply to the monitoring of business email accounts. Considerable risks could arise from violations of the law, up to and including possible criminal liability pursuant to sec. 206 I *StGB* or secs. 44 I, 43 II *BDSG*.[47] If the recommendations specified in the above checklist are taken into account, these risks can be significantly reduced or even ruled out. Moreover, companies should review and, if necessary, thoroughly revise existing usage rules or works agreements relating to the handling of emails within the company.

A. Approach if private use is prohibited

If companies wish to access their employees' business emails in a legally secure manner, they should, if possible, prohibit the private use of company accounts. In this case, electronic communication in the company is treated similarly to business letters. As the right to privacy of the employees concerned is usually only affected to a minor extent in such cases, the weighing up of interests will mostly favor the employer. However, in this case, too, the employer should clarify as a matter of urgency which monitoring measures it reserves the right to implement.

B. Approach if private use is permitted

In practice, it is often not expedient to prohibit the private use of business emails in many cases. According to the view taken by most supervisory authorities for data protection and probably still the majority of the specialist literature, risks of criminal liability can be ruled out in the case of email monitoring due to sec. 206 I *StGB* at most by carefully drafted provisions on the use of corporate email systems.[48] In these cases, employers should only allow private use by those employees who have consented to appropriate monitoring of their electronic communication.

---

47 Cf. e.g. *BGHSt* 58, 268 = NJW 2013, 2530 with comments by Tim Wybitul, ZEITSCHRIFT FÜR DATENSCHUTZ, 509 (2013).

48 As also stated *by* Michael Walther & Mark Zimmer, *Mehr Rechtssicherheit für Compliance Ermittlungen,* BETRIEBS-BERATER, 2933, 2937 (2013).

The company can certainly instruct employees not to store sensitive or intimate content on corporate IT systems by issuing guidelines or works agreements. It can also order employees not to use company computers for any content that the employer is not supposed to monitor. If employees store private content despite this prohibition, it must be clear to them that they cannot invoke the fact that they expected the company not to access their data. This applies in particular if the employer expressly reserves the right to make random checks or to implement monitoring if there is a firm suspicion of breaches of duty.