BRANDI
RECHTSANWÄLTE

EMPLOYER ACCESS TO EMPLOYEE E-MAIL ACCOUNTS

Information on data protection I December 2022

Introduction

A large number of employees have a business e-mail account for the performance of their duties. Occasional access to these e-mail accounts is a relevant issue for many companies. In practice, the question frequently arises as to whether or in which cases and to what extent the employer may access the business e-mail accounts of its employees and what requirements must be observed in this regard.

Of particular practical relevance here is, on the one hand, the case where access to an employee's e-mail box is required in order to be able to process the employee's business correspondence in the event of the employee's absence. On the other hand, in certain cases employers have an interest in checking whether an employee's e-mail account is being misused, for example for private communication during working hours or even for passing on business secrets.

Legal bases

Any data processing – and accordingly also access to an e-mail box – is generally only permissible if it can be based on a legal basis. In this respect, the prohibition with reservation of permission anchored in Article 6 (1) of the GDPR applies. Since, contrary to various considerations in the past, there is currently no comprehensive employee data protection law, the general data protection provisions of the GDPR and the BDSG as well as the special provision of Section 26 BDSG ("Data Processing for the Purpose of The Employment Relationship") must be applied when processing employee data.

Purposes of the employment relationship, performance of a contract and legitimate interests

The legal basis for accessing an employee's e-mail box is, in particular, Section 26 (1) (1) of the BDSG and Article 6 (1) (1) (b) of the GDPR. Pursuant to Section 26 (1) (1) of the BDSG, personal data of employees may be processed for purposes of the employment relationship if this is necessary for the decision on the establishment of an employment relationship or, after the establishment of the employment relationship, for its implementation or termination or for the exercise or fulfillment of the rights and obligations of the employees' representation of interests resulting from a law or a collective agreement, a works agreement or a service agreement. The general provision pursuant to Article 6 (1) (1) (b) of the GDPR is relevant outside the performance of the employment relationship and covers data processing for the performance of a contract with the data subject. Accordingly, if there is an operational requirement for access that relates to the employee's employment relationship – such as the representation and processing of open tasks in the event of absence – Section 26 (1) (1) of the BDSG or Article 6 (1) (1) (b) of the GDPR can be used as the legal basis.

If a person does not fall within the scope of Section 26 of the BDSG due to a lack of employee status within the meaning of Section 26 (8) of the BDSG (e.g. a managing director), Article 6 (1) (1) (f) of the GDPR may also be considered as a further legal basis in addition to Article 6 (1) (1) (b) of the GDPR. According to Article 6 (1) (1) (f) of the GDPR, data processing is permissible if the legitimate interest of the controller, i.e. the employer, in the data processing outweighs the interests or fundamental rights and freedoms of the data subject. Consequently, the interests of the parties involved must be weighed in the specific case. If access is necessary, for example, to maintain business operations, an overriding legitimate interest will generally be assumed.

Detection of a criminal offense

If the e-mail box is to be accessed in order to uncover a criminal offense, the special permissive circumstance of Section 26 (1) (2) of the BDSG may be invoked. According to this, however, data of employees may only be processed for the purpose of uncovering criminal offenses if factual indications to be documented give rise to the suspicion that the data subject has committed a criminal offense in the employment relationship, the processing is necessary for the purpose of uncovering the offense, and the employee's interest worthy of protection does not prevail. If there is a reasonable suspicion of a criminal offense committed by an employee in the employment relationship, access may be permissible pursuant to Section 26 (1) (2) of the BDSG.

Consent

Another possible legal basis is the consent of the data subject to access the e-mail box. It should be noted, however, that relying on consent in the employment relationship is not without problems. Pursuant to Section 26 (2) of the BDSG, high demands must be placed on the voluntary nature of consent due to the relationship of dependency between employee and employer. The extent to which obtaining the data subject's consent is actually practicable is likely to depend, as a rule, on the reason for the desired access. If the employee is guilty of misconduct, he or she is unlikely to give his or her consent to access, whereas this is likely to be the case in the event of a substitution.

Works agreement

Finally, the conclusion of a works agreement to justify access to an employee's e-mail account may also be considered. According to Section 26 (4) of the BDSG, the processing of personal data, including special categories of personal data of employees for purposes of the employment relationship, is also permitted on the basis of collective agreements. It may be advisable to conclude a works agreement if further points, such as the exclusion of private use and

the specific procedure in the event of access, are to be regulated in a legally secure manner within the framework of the agreement, taking into account the interests of the employer, employee and works council, and uncertainties are to be avoided.

Principle of proportionality and data minimization
In principle, a proportionality test, i.e. a weighing of the interests of the employer and the interests of the employee, is required for every access, regardless of the specific legal basis. In addition, the principle of data minimization according to Article 5 (1) (c) of the GDPR must be observed. In this respect, the employee's e-mails may not be accessed indefinitely, but only to the extent necessary.

The principle of proportionality may also give rise to an obligation on the part of the employer to inform the employee concerned – if necessary after the fact – about access to his or her e-mail box.

(Permitted) private use of the e-mail account

A particular problem arises when employees are permitted or at least tolerated to use their e-mail accounts for private purposes. In this case, it is questionable whether, in addition to the data protection provisions of the GDPR and the BDSG, the employer must also observe the secrecy of telecommunications pursuant to Section 3 of the Telecommunications Telemedia Data Protection Act (TTDSG). The question also arises as to the cases in which permitted private use is to be assumed.

Applicability of the secrecy of telecommunications
According to some data protection supervisory authorities, the secrecy of telecommunications also applies in employment relationships if employees are permitted private use of their e-mail accounts. In this context, the employer is classified as a provider of telecommunications services, which means that the employer must observe the secrecy of telecommunications and may not access the e-mail accounts of its employees. Providers of telecommunications services may only view the transmitted content if this is necessary for the provision of the service, including the protection of the technical systems required for this purpose. However, this cannot be assumed either in the case of absence for the processing of business correspondence or in alleged cases of misuse, so that access to the e-mail box would, according to this view, fundamentally violate the secrecy of telecommuniactions and would therefore be inadmissible.

By contrast, the Regional Court of Erfurt (LG Erfurt, judgment of April 28, 2021, Ref. 1 HK O 43/20) and the Regional Court of Krefeld (LG Krefeld, judgment of February 7, 2018, Ref. 7 O 175/17) reject the applicability of telecommunications secrecy in the case of permitted private use and consider access to employees' e-mail accounts to be permissible in certain cases. In accordance with the statements of the courts, the lawfulness of the inspection is governed exclusively by the provisions and principles of data protection law. Various other courts have already ruled in the past, such as the Regional Court of Erfurt and the Regional Court of Krefeld (see, among others, LAG Berlin-Brandenburt, judgment of January 14, 2016, Ref. 5 Sa 657/15, LAG Niedersachsen, judgment of May 31, 2010, Ref. 12 Sa 875/09). Nevertheless, the case law on this issue is not uniform (different opinion: LAG Hessen, judgment of September 21, 2018, Ref. 10 Sa 601/18, LAG Rheinlad-Pfalz, judgment of December 4, 2017, Ref. 3 Sa 143/17) and there is no conclusive supreme court clarification of the issue. If an employer accesses an e-mail box even though it is protected by the secrecy of telecommunications, the employer may be liable to prosecution under Section 206 (1) of the Criminal Code. In addition, there is the threat of severe fines.

Even if one opposes the application of telecommunications secrecy, however, this does not mean that access is possible at any time without further ado; the data protection principles already described must be taken into account in any case. If employees are permitted to use their e-mail accounts privately, this means that the employer's interest in access is offset by the employee's important interest in protecting his or her privacy, and these must be taken into account to a sufficient extent when weighing the interests.

Permitted private use
A business e-mail account is, in principle, a business resource. If such equipment is made available to employees without further information, the principle applies that it may only be used for business purposes and that private use is not permitted, so that the scope of application of telecommunications secrecy is generally not opened up. However, something else may apply if the employees nevertheless use the e-mail account privately, the employer is aware of this and does not prevent the behavior of its employees. The scope of application of the secrecy of telecommunications can be opened not only if the employer has expressly permitted private use, but also if he merely tolerates it, depending on the opinion held. If, however, an employee uses the e-mail account privately in violation of instructions, there is no interest of the employee worthy of protection.

To avoid uncertainties, it is advisable to regulate the topic explicitly within the company – for example, within the framework of a data privacy & IT policy. At best, employees should be expressly prohibited from using their business e-mail accounts privately until the issue has been conclusively clarified by the highest court and by law, in order to reliably exclude the applicability of telecommuniactions secrecy and not to fundamentally rule out any access rights in individual cases. After all, such a ban does not mean that employees may not occasionally send private e-mails via a webmail service or their private smartphone. If private use of the company e-mail account is nevertheless to be permitted, companies should alternatively obtain the express consent of the employees to be released from the restrictions of telecommunications secrecy.

Access in the absence of an employee

If an employee falls ill or is absent for another reason (for example, vacation or parental leave), sometimes for a longer period of time, and if no precautions have been taken in advance for the specific case, it is often necessary for the employer or other employees of the company to access the respective e-mail box in order to maintain operational processes. In particular, if the absent employee communicates mainly with external persons via his or her e-mail account, access to the e-mails and a review of the respective correspondence may be necessary in order to be able to follow up on currently relevant topics on the company side and to process them promptly.

Access during temporary absence
In order to anticipate any need for access and the associated problems, it is advisable to define general rules for the absence of employees in advance. This applies in particular to planned absences such as vacation or parental leave. The mildest means in this respect is the setting of an automatic absence note by the employee himself. If this is not sufficient, for example, due to the employee's activities or the documents and inquiries received via the e-mail account, e-mails may also be forwarded to the absent employee's deputy and must be set up by the employee prior to his or her absence.

In the case of unforeseeable absences, such as in the event of illness, such specifications are generally not sufficient, as it is often no longer possible for the employee to set the absence note or set up e-mail forwarding due to lack of access. In this case, the employer may need to access the employee's e-mail account.

Access and the subsequent setting up of an absence note can then be based on Section 26 (1) (1) of the BDSG or Article 6 (1) (1) (b) of the GDPR or, in the case of persons who do not fall under the definition of employees, on Article 6 (1) (1) (f) of the GDPR. The same applies to the ordering or setting up of e-mail forwarding and access to e-mails already received in the meantime, insofar as the sifting and further reading are necessary for the deputy (further) processing of tasks or the maintenance of business operations. If there is a works agreement with corresponding regulations for absences, this can be used as the legal basis for access. In addition, the employee's consent may also be considered.

If an e-mail box is accessed in the event of a deputy, care must also be taken to ensure that no third party (e.g. the deputy) uses the e-mail box of the absent employee, as otherwise it will no longer be possible to trace who wrote the e-mails. Instead, only the user's own mailbox should be used for the deputy further processing of open tasks.

Access after an employee leaves

Even after an employee has left, his or her e-mails may not be accessed without further ado. In this case, a legal basis is also required for data processing. It is therefore advisable to regulate the issue in advance as part of the employment contract or a separate agreement so that no information relevant to business operations is lost. It can be agreed, for example, that the employer may access the employee's e-mails after the employee leaves or forward them to the colleague who is now responsible. Alternatively, an obligation on the part of the employee to hand over open tasks upon leaving and to file documents and correspondence required for business operations in a specific storage location may also be considered. In all other respects, reference can be made to the comments on temporary absence with regard to the legal basis.

Access in the event of suspected abusive behavior

If the employer suspects that an employee is misusing his or her company e-mail account, for example through excessive private use, the disclosure of business secrets or even the sale of customer data, the company often wishes to access the employee's e-mail account in order to investigate the suspicion and clarify the facts. In particular for these cases, which are sometimes the subject of disputes, it is advisable to conclude a corresponding works agreement in order to be able to act swiftly and with legal certainty.

If there is a concrete suspicion that an employee has committed a criminal offense within the scope of his or her employment – in this respect, the disclosure of business secrets and confidential information or the sale of customer data may come into consideration – access may also be justified in accordance with Section 26 (1) (2) of the BDSG, provided that the requirements of the standard are met. Specifically, the suspicion must first relate to a criminal offense, this must have been committed in the employment relationship, there must be factual indications for the suspicion and the access must be necessary to solve the criminal offense. Finally, the conflicting interest must be weighed against each other.

If, however, the employer merely assumes that an employee has violated his or her contractual duties, for example, through excessive private use, Section 26 (1) (2) of the BDSG cannot generally be invoked due to the lack of a criminal offense. In this case, recourse to Section 26 (1) (1) of the BDSG is again necessary. However, additional problems may arise if the employer already assumes private use, which may shift the balance of interests in the employee's favor due to the protection of the employee's privacy. In view of the sensitivity of the subject and its susceptibility to dispute, the case should first be examined by the data protection officer.

Procedure for accessing the e-mail account

If access to the e-mail box is covered by a legal basis, the question then arises as to how to proceed with the access in concrete terms. In principle, the company should first take into account that not only the relevant legal basis in a specific case, but also the further procedure depend on the respective circumstances of the individual case. In order to ensure that data protection regulations are complied with and the interests of the employee are adequately protected, it is generally advisable to proceed according to the "multiple-eyes principle". If there is a works council, it is generally advisable to involve it. It is also advisable to obtain an assessment of the situation from the data protection officer in advance and to coordinate the specific procedure with him, even if he does not necessarily have to directly accompany the access in the end. For evidence purposes, access should also be logged in detail and the respective considerations regarding access, in particular the weighing of interests, should be documented.

Conclusion

Access to employees' e-mail accounts raises many questions and is not unproblematic, especially if private use cannot be ruled out with certainty. It therefore makes sense to establish clear rules for accessing an e-mail box in advance in order to avoid uncertainties and any potential for disputes. In this respect, it is particularly advisable to conclude a corresponding works agreement and a data protection & IT policy, which can also be used to regulate other issues relating to the use of IT systems.

If access to an employee's e-mail account is actually required in the course of everyday work, data protection-compliant handling of the data should always be ensured by appropriate safeguards, such as the use of the "multiple-eyes principle" and comprehensive documentation. In view of the sensitivity of the topic and the possible consequences of unauthorized access, it is also advisable to coordinate the specific procedure with the data protection officer.

Christina Prowald

Contact:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Christina Prowald
Research Associate

T +49 521 96535 - 890
F +49 521 96535 - 113
M christina.prowald@brandi.net