KNOW-HOW

Gleiss Lutz

17.04.2018

COMPLIANCE & INVESTIGATIONS

INTERNAL INVESTIGATIONS AND DATA PROTECTION

With the coming into force of the EU's General Data Protection Regulation and at the same time the new version of the Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG) on 25 May 2018, the rules governing the processing of data during internal investigations will also be put on a new footing. The German legislator has made use of the possibility opened up in Article 88(2) General Data Protection Regulation for Member States to provide for national statutory rules to apply to the protection of employees' personal data in the form of section 26 Federal Data Protection Act.

The new provision is patterned on section 32 Federal Data Protection Act, old version, and should according to the legislator specifically not lead to any legal change as compared to the previous legal situation, which has been fleshed out in case law.

Effects on preventive compliance investigations

This means for preventive compliance investigations not based on a specific suspicion of a certain person having committed a criminal offence that they can now be underpinned by section 26(1), sentence 1 (previously section 32(1), sentence 1) Federal Data Protection Act since the special provision in section 26(1), sentence 2 (previously section 32(1), sentence 2) for uncovering criminal offences does not, as lex specialis, exclude cases in which other compliance violations such as administrative offences or violations of internal rules are to be investigated.

Investigative measures that have a preventive aim are therefore also possible under the new law. In the diction of the General Data Protection Regulation, they are permissible under Article 6(1)(f) – processing for the purposes of the legitimate interests pursued by the controller or by a third party – provided that their necessity has been demonstrated and the interests or fundamental rights and freedoms of the data subject do not override the legitimate interests of the employer.

The strict principle of proportionality, according to which the measure must be suitable, necessary and appropriate, that is emphasised in the case law of the Federal Labour Court and the European Court of Human Rights also continues to apply in this regard.

When looking at necessity, it must be checked whether the measure is the least stringent among several equally suitable measures. When checking whether a measure is appropriate, the legitimate interests of the employer must be weighed up against the interests of the employee concerned.

Consequently, mass comparisons of data, indiscriminate fishing expeditions and extensive ongoing monitoring activities should be avoided in future too. When for example analysing an internet browser to monitor compliance with a ban on internet use, usage data and metadata should therefore at best be scrutinised at random in terms of how, when and for how long the internet is used. The period of time for which such data is stored for documentation purposes should also be restricted with a view to intended further use (e.g. warning, disciplinary action).

A further legal basis for processing data is laid down in Article 6(1)(a) General Data Protection Regulation, which stipulates that data may be processed if the data subject has given his/her consent. The revised section 26(2) Federal Data Protection Act contains extensive provisions in this regard that ultimately mean that consent has only been validly given by the employee of his/her own free will if there is a legal or economic benefit for the employee

or if the employee and the employer are pursuing similar interests. The pursuit of similar interests may come into question in cartel cases, in particular, in which the company files a leniency application in which it claims the benefits of the application in favour of the employee concerned as well. In the case of other internal investigations, the question is how these could be described as "only beneficial" for the employees.

Effects on investigatory investigations

Section 26(1), sentence 2 Federal Data Protection Act now provides the relevant permission for investigations that are based on a suspected criminal offence. As was already the case under the "old regime", there must be a reasonable suspicion within the meaning of section 152 German Code of Criminal Procedure; this must not be subject to overly stringent requirements, however.

Sufficient factual indications that an offence has been committed are deemed to exist if the information and indications available prior to the data processing contain a factual core that makes it appear possible that criminal offences have been committed. It is not necessary for any evidence that could be used in court to be available at this stage. Indicative and circumstantial evidence as well as specific facts outside the scope of the suspected crime may suggest that a criminal offence has been committed. These are sufficient even if conclusions are initially based on conjecture and have been logically deduced or are to be derived based on experience in criminalistics and criminology. In contrast, mere rumours, prejudices or hunches are not sufficient to establish a reasonable suspicion under the law of criminal procedure. This means that in the case of whistleblower information, efforts should generally be made to check whether this is plausible and to verify this based on other information before the relevant data is accessed.

Moreover, the reasonable suspicion does not initially have to be directed against an individual, but must be directed at least against a specific, definable group of persons. In companies, external factors such as the restriction of access to certain areas, the times of access and use, for example where shift work is involved, or other aspects may be used to define the relevant group.

In investigations based on suspected criminal offences, this reasonable suspicion must be documented in writing together with the corresponding factual basis and must be taken into account when weighing up the various interests concerned. Such a weighing up of the interests involved must also be carried out within the framework of section 26(1), sentence 2, since even a reasonable suspicion that an offence has been committed does not automatically mean that data can be used without restriction.

Although it will usually be necessary to investigate such a suspicion for the purpose of carrying out or terminating the employment contract, the suspicion that a criminal offence has been committed nevertheless does not release the company from the need to assess the appropriateness of the data use in relation to the data subject's right to privacy.

Investigations on the basis of the Money Laundering Act

Investigations by credit and financial institutions on the basis of the German Money Laundering Act (Geldwäschegesetz) and to prevent fraud (pursuant to section 25h(3) German Banking Act and section 15(3), no. 2 in conjunction with (5) German Money Laundering Act) are moreover to be based on the criterion laid down in Article 6(1)(c) – compliance with a legal obligation to which the controller is subject – irrespective of the question of whether the investigation is to be attributed to the preventive or investigatory work to be carried out by the institution's central office.

As far as the prevention of money laundering is concerned, it could also be argued that the obliged persons are carrying out a task that is, pursuant to Article 6(1)(e) General Data Protection Regulation, in the public interest, since the law has in this regard transferred a very wide range of tasks to the obliged persons as private entities.

Investigations for purposes not related to the employment relationship

Finally, it should be pointed out that section 26(1) Federal Data Protection Act constitutes lex specialis when it comes to the employment relationship, whereas the other requirements laid down in the General Data Protection Regulation and the Federal Data Protection Act continue to apply in addition to data processing for purposes not related to the employment relationship. If, therefore, an investigation is not being carried out in an employment context but instead serves the purpose of, for example, averting attempts to perpetrate fraud by third parties or of asserting and enforcing legal claims following the discovery of such fraud, the permission criteria in Article 6(1)(c) and (f) General Data Protection Regulation can be used as a basis. This then also makes it possible to access the data of a user employed by the company who has, for example, communicated with the external suspect.

Access to employee’s e-mail accounts

Access to employees' e-mail accounts as part of internal investigation measures is still not explicitly regulated. Thus, it remains unclear until further notice whether the employer is subject to the restrictions of telecommunications secrecy within the meaning of sections 88 Telecommunications Act (Telekommunikationsgesetz), 203 German Criminal Code (Strafgesetzbuch) in case of permitted private use of company e-mail access, with the result that he would de facto be denied any access to the employees' e-mails. In order to avoid the resulting uncertainties and to be on the safe side in terms of data protection law, it is essential to clearly regulate the handling of e-mails in the company and either completely exclude private use or make it dependent on the employees' written consent to such access by the employer for legitimate company purposes, which would be permissible on the legal basis outlined above without permission for private use. The fact that such a consent is possible and effective, because it gives the employees an advantage by allowing private use, was expressly emphasised by the legislator in the explanatory statement to section 26(2) BDSG.

Works council’s co-determination rights

It should also be pointed out that in the context of the protection of employee data, the works council’s co-determination rights under employment law remain unaffected and, as far as the agreement of collective provisions is concerned, section 26(4) Federal Data Protection Act makes it possible to lay down corresponding works agreements, for example governing electronic compliance checks.

EXPERTISE

Banking and Finance
Compliance & Investigations
Data Protection

LAWYERS

Dr. Dirk Scherp

Dr. Christian Hamann