

Information Technology
& Communications
Germany

August 2018

GDPR – German data protection authorities establish new rules for whistleblowing hotlines: Call for action

The coming into force of new EU-wide privacy legislation means German companies should review, and likely implement, changes to any existing whistleblowing hotlines offered to their employees. In light of the implementation of the General Data Protection Regulation ("GDPR"), the German data protection authorities ("German DPAs") have changed their position on, amongst others, how employees submit whistleblowing reports anonymously. The German DPAs recently issued guidance on this point¹:

The general EU position before the GDPR was implemented was that whistleblowers were not encouraged to file anonymous reports. We note that, in some EU countries, such as Portugal, anonymous reporting was in fact prohibited. The Guidance, in light of the implementation of the GDPR, reverses this position and now provides that employees must be encouraged to submit reports anonymously. The Guidance also provides that, when an employee wishes to identify himself as the whistleblower, the employee must be informed that his/her identity will be disclosed to the individuals mentioned in the report and that the employee's consent is required for this disclosure. Art. 14 GDPR provides that the individuals mentioned in the report must be informed about the whistleblowing report, including the identity of the whistleblower as the source of the personal data.

Details of the German DPAs position:

- a) Art. 14 GDPR requires the controller to inform the data subjects when personal data have not been collected directly from the data subject. As part of Art. 14 GDPR, when informing the data subject about the data collection, the controller must include details about the source of the personal data (Art. 14 (2)(f) GDPR). The German DPAs interpret this as a requirement to identify the whistleblower vis-à-vis the individuals mentioned in a report, in particular the accused person, as the source of the data, by disclosing the name of the whistleblower.
- b) Consequently, the company to which the disclosure is made can no longer provide an undertaking to the whistleblower that his/her identity will be kept confidential. The company will need to explicitly disclose that the person as the source of the disclosure will need to be disclosed by name, to the accused individual.

Our Expertise
**Information Technology &
Communications**



¹ The **Guidance**: Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz, available in German here: https://datenschutz.saarland.de/fileadmin/datenschutz/dsk_entschliessungen/95/Orientierungshilfe-Whistleblowing-Hotlines.pdf

Hot Topics

- c) The Guidance from the German DPAs further determines that – with respect to the whistleblower – there is no statutory justification ground which permits the disclosure of the whistleblower's name to the accused person. The German DPAs apparently do not recognize Art. 6(1)(c) GDPR (where processing is necessary for compliance with a legal obligation) or the balancing of interest test in Art. 6(1)(f) GDPR as the legal basis for the disclosure of the whistleblower's name pursuant to Art. 14(2)(f) GDPR to the accused person. Therefore, the whistleblower's consent shall be required.
- d) As a result, whistleblowers have two options when submitting a whistleblowing report: (1) Submitting the report only anonymously, or (2) identifying themselves and consenting to the company disclosing their identity to the accused when submitting the report. Companies shall strongly encourage option (1) – anonymous reporting. The German DPAs have thus reversed their position on anonymous reporting. Employees were previously encouraged to identify themselves. This was arguably in order to reduce the risks of unfounded complaints, to make the subsequent investigation easier, and to allow follow-up questions to be posed to the whistleblower. Thus, previously, companies had to commit to keep the identity of the whistleblower confidential as far as possible.
- e) If the whistleblower decides to give consent to the company to disclose his identity to the accused person, the whistleblower retains the right to withdraw his consent at any time, as per Art. 7(3) GDPR. However, the whistleblower must be informed about this right when submitting the report, and must be further informed that a withdrawal after one month would typically be too late in order to avoid the disclosure of his identity to the accused. This is because Art. 14(3) GDPR requires that the accused needs to be informed about the whistleblowing report, including the source, at the latest within one month after the personal data was obtained.
- f) Beyond the issue of anonymous reporting, the German DPAs state that compliance reports relating to the well-known subject matters, which were confirmed by the Art. 29 Working Party and the German DPAs in 2006 and 2007 respectively, continue to be permissible. These include subject matters relating to financial issues (such as fraud, internal accounting controls, auditing matters, corruption and bribery, banking and financial crimes, and insider trading), human rights violations, and environmental concerns. Furthermore, the German DPAs consider the collection of personal data via a whistleblowing hotline permissible if it relates to an alleged violation of the law against equal treatment. The German DPAs argue that the processing of such personal data is permissible based on Art. 6 (1)(f) GDPR (balancing of interest test) because the investigation into those alleged violations could hinder legitimate law enforcement activities, damage claims, and reputational harm for the company. Unfortunately, the German DPAs do not discuss whether these arguments could also be applied to other subject matters such as violations of data privacy law, anti-trust law, or HR harassment cases, which could also result in damage claims and severe reputational harm.
- g) Unfortunately, the German DPAs do not discuss whether Art. 10 GDPR applies to whistleblowing hotlines. Art. 10 GDPR provides that personal

Hot Topics

data relating to criminal offences and related security measures may only be processed, amongst other cases, when authorized by EU or Member State law. In our view, the fact that the German DPAs do not mention Art. 10 GDPR could imply that the German DPAs do not consider reports on alleged criminal offences as covered by Art. 10 GDPR.

- h) Further, the German DPAs consider whistleblowing hotlines as a high risk processing activity requiring a data protection impact assessment pursuant to Art. 35 GDPR.

Open Issues:

Implementing the Guidance will create challenges for companies. The Guidance is also open to criticism on several grounds. For example:

- a) The practical implementation of the Guidance will be challenging. As an illustration, in order to implement the anonymous reporting system and the 'consent requirement' when non-anonymous reporting occurs, companies should only allow reporting via an online intake form. This is because reports via email would typically always disclose the identity of the whistleblower via the email address used to send the report, and reports via email or telephone would require additional measures to allow the collection of documented, written, consent in case the reporter wants to disclose his identity.
- b) Furthermore, it is unclear how a company should proceed if it receives a potential compliance concern via email, i.e. outside the reporting channel of the whistleblowing hotline. Is the company in this case required to follow up with the reporter in order to obtain the consent? Or, is the company then prevented from investigating the case? What if the reporter refuses the consent? If the company does not disclose the name of the whistleblower to the accused, it would violate Art. 14 GDPR. If the company discloses the name of the whistleblower to the accused, it would violate Art. 6 GDPR because the company does not have a legal basis for the disclosure, i.e. the consent of the whistleblower.
- c) It is unclear why the German DPAs did not further elaborate on their interpretation of Art. 14(f) GDPR. Why do they interpret "information about the source from which the personal data originated" as providing the identity of the source? Wouldn't it be sufficient to disclose the name as "a reporter who contacted the whistleblowing hotline" or "another employee"?
- d) Another concern is why the German DPAs do not discuss exceptions. For example, Art. 14(5)(b) GDPR provides an exception if the provision of such information proves impossible, in particular in so far as the disclosure requirements are likely to render impossible or seriously impair the achievement of the processing's objective. One could argue that, without confidentiality, internal misconduct will not be reported as employees fear retaliation. Another exception could be provided by Sec. 29 of the German Federal Data Protection Act. This provides that the information obligation of Art. 14 GDPR shall not apply as far as this would require the disclosure of information which, by its nature, must be kept secret, in particular because of overriding legitimate interests of a third party. One could argue that the whistleblower has an overriding legitimate interest that his identity not be disclosed.

Hot Topics

- e) Why did the German DPAs not liaise with the other European data protection authorities on this issue, in light of Art. 60 and 63 GDPR and the overall objective of the GDPR to harmonize the application of data privacy laws in Europe?

Compliance with the new Guidance will thus pose practical challenges. It remains to be seen whether the European Data Protection Board will shortly pick up on this issue, and whether European-wide guidelines which also consider the practical implementation of these provisions will be released.



Julia Kaufmann LL.M.
julia.kaufmann@bakermckenzie.com



Dr. Katia Helbig LL.M.
katia.helbig@bakermckenzie.com



Prof. Dr. Michael Schmidl LL.M.
michael.schmidl@bakermckenzie.com



Dr. Holger Lutz LL.M.
holger.lutz@bakermckenzie.com

Baker & McKenzie - Partnerschaft von Rechtsanwälten, Wirtschaftsprüfern und Steuerberatern mbB

Berlin

Friedrichstrasse 88/Unter den Linden
10117 Berlin
Tel.: +49 30 2 20 02 81 0
Fax: +49 30 2 20 02 81 199

Frankfurt am Main

Bethmannstrasse 50-54
60311 Frankfurt / Main
Tel.: +49 69 2 99 08 0
Fax: +49 69 2 99 08 108

Dusseldorf

Neuer Zollhof 2
40221 Dusseldorf
Tel.: +49 211 3 11 16 0
Fax: +49 211 3 11 16 199

Munich

Theatinerstrasse 23
80333 Munich
Tel.: +49 89 5 52 38 0
Fax: +49 89 5 52 38 199

www.bakermckenzie.com

Get Connected:



This client newsletter is prepared for information purposes only. The information contained therein should not be relied on as legal advice and should, therefore, not be regarded as a substitute for detailed legal advice in the individual case. The advice of a qualified lawyer should always be sought in such cases. In the publishing of this Newsletter, we do not accept any liability in individual cases.

Baker & McKenzie - Partnerschaft von Rechtsanwälten, Wirtschaftsprüfern und Steuerberatern mbB is a professional partnership under German law with its registered office in Frankfurt/Main, registered with the Local Court of Frankfurt/Main at PR No. 1602. It is associated with Baker & McKenzie International, a Verein organized under the laws of Switzerland. Members of Baker & McKenzie International are Baker McKenzie law firms around the world. In common with terminology used in professional service organizations, reference to a "partner" means a professional who is a partner, or equivalent, in such a law firm. Similarly, reference to an "office" means an office of any such law firm.