Baker McKenzie.

Hot Topics

Information Technology & Communications
Germany

January 2019

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

Update (January 2019): This client alert was published in August 2018. In the meantime, the German data protection authorities have reacted to the criticism and comments that were raised in relation to their new rules for whistleblowing hotlines and released an updated version of their guidelines on November 14, 2018. The updated guidelines now specifically address the question of potential exemptions from the information obligation pursuant to Art. 14 GDPR. Unfortunately, the guidelines still lack specific examples on when exactly the German data protection authorities consider those exemptions to be applicable. Please see I.b and II.d for details.

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 point[1]:

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.

I. 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

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

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) **Update (January 2019)**: An updated version of the Guidance - released in November 2018 - now expressively addresses several exemptions to the general information obligation.

- According to the German DPAs, the obligation to inform the individuals mentioned in the report can be postponed as long as there is a significant risk that the information endangers the ability of the company to effectively investigate the report or to collect the required evidence. This exemption is based on Art. 14(5)(b) GDPR which provides that the information obligation shall not apply where and insofar as the provision of such information proves impossible or would involve a disproportionate effort, in particular where the information is likely to render impossible or seriously impair the achievement of the objectives of that processing. However, the German DPAs also expressively state that the information obligation must still be complied with at a later stage, namely once informing the individual does not pose a threat to the investigation anymore.

- Furthermore, the German DPAs mention that no information obligation exists in case of Art. 14(5)(d) GDPR which provides an exemption where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

- Lastly, the German DPAs address Sec. 29(1) sentence 1 of the German Federal Data Protection Act according to which the obligation to provide information to the data subject shall not apply as far as meeting this obligation would disclose information which by its nature must be kept secret, in particular because of overriding legitimate interests of a third party.

c) Since the German DPAs take the view that the identity of the whistleblower must in general be disclosed to the reported person, the company to which the disclosure is made can no longer provide an undertaking to the whistleblower that his/her identity will be kept fully 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. However, the German DPAs still recommend informing the reporting person that his/her identity will - with the exception of the information to the reported data subject - be treated confidentially during the entire investigation.

d) 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.

e) 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.

f) 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.

g) 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.

h) Unfortunately, the German DPAs do not discuss whether Art. 10 GDPR applies to whistleblowing hotlines. Art. 10 GDPR provides that personal 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.

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

II. 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 - provided no exemption applies - 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) **Update (January 2019)**: While the German DPAs mention the exemption of Sec. 29 of the German Federal Data Protection Act (cf. above), it remains unclear when and under which circumstances they deem such provision to be applicable. In our view there are robust arguments that the whistleblower has generally an overriding legitimate interest that his identity is not disclosed.

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

Duesseldorf
Neuer Zollhof 2
40221 Duesseldorf
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: