Julia Kaufmann / Katja Häferer / Kerstin Grimhardt*

The new EU Whistleblowing Directive

Considerations from a German employment and data protection law perspective

Recently, the EU reached another milestone in the field of whistleblowing: In December 2019, the Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law ("Whistleblowing Directive") entered into force. Member States are required to transpose the Whistleblowing Directive into national law and to apply such national laws as of 17 December 2021. Such national laws will require, among others, companies with more than 50 employees to implement internal compliance reporting channels and to provide protection for individuals, most importantly employees, who report a compliance concern via the internal or external reporting channels provided for by the Whistleblowing Directive.

The respective national laws implementing the Whistleblowing Directive will have an impact on how reporting systems will be set up in the future, what type of protection employees will enjoy and how data protection law requirements are addressed in this context. EU Data Protection Authorities will very likely need to amend and update their existing guidelines on the processing of personal data in the context of whistleblowing hotlines. We expect changes, in particular, on the issue around anonymous reporting, on the permissible subject matters that can be reported, and on the internal responsibility for handling reports.

I. Scope and Purpose

1 All companies in the EU, irrespective of the size, are required to ensure that whistleblowers are protected against any form of retaliating measures. Furthermore, companies in the EU with 50 or more employees[1] as well as most companies in the public sector will be required to implement an internal reporting and follow-up system enabling employees and certain other individuals to report compliance concerns (Art. 8 (3) and 8 (9) of the Whistleblowing Directive). National laws may expand this obligation of implementing such a reporting system to companies with fewer than 50 employees following a risk assessment (Art. 8 (7) of the Whistleblowing Directive).

1. Purpose

2 The primary purpose of the Whistleblowing Directive[2] is to protect whistleblowers who have reported a breach in accordance with the rules set out in the Whistleblowing Directive[3]. Companies will be required to refrain from any form of actual, threatened or attempted work-related retaliation against the whistleblower (Art. 19 of the Whistleblowing Directive). The national laws implementing the Whistleblowing Directive will therefore need to ensure, in particular, that whistleblowers are protected against termination of employment, negative impact on promotions or salary, unjustified negative performance assessment, transfer and change of workplace, harassment or discrimination.

The protection to be granted by national laws will expand to 3
third parties who are connected to the whistleblower such as the whistleblower's colleagues or relatives provided they could also suffer work-related retaliation (Art. 4 (4) (b) of the Whistleblowing Directive).

National laws will need to ensure such protection of the whis- 4
tleblower if (1) the whistleblower had reasonable grounds to believe that (a) the information reported about the potential breach was true at the time of reporting and (b) such information was in scope of the Whistleblowing Directive and if (2) the whistleblower used the reporting channels foreseen by the Whistleblowing Directive (Art. 6 (1) of the Whistleblowing Directive). For example, a whistleblower shall not be considered to have breached confidentiality obligations if he/she had reasonable grounds to believe that the reporting of such information was necessary to reveal the breach of law. Likewise, whistleblowers are protected if they had reasonable grounds to believe that the reported information referred to any of the subject matters covered by the Directive (as further outlined below) even if they did in fact not refer to those subject matters.

2. Protected Subject Matters

As of now, EU Data Protection Authorities have taken the po- 5
sition that whistleblowing systems must be restricted to certain permissible subject matters. For example, the German Data Protection Authorities have reconfirmed in January 2019[4] that a whistleblowing system may accept reports only if the report relates to one of the following subject matters: financial issues (e.g, fraud, internal accounting controls, auditing matters, corruption and bribery, banking and financial crimes, insider trading), human rights violations, and environmental concerns. Other Data Protection Authorities in the EU have established similar restrictions. In all other cases, reports are either not per-

* The authors express their thanks to *Tobias Kalb*, law clerk at Baker McKenzie, for his valuable support.

1 For companies with less than 250 employees, the obligation to establish such an internal reporting system does not apply until 17 December 2023.

2 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L1937&from=EN.

3 https://www.consilium.europa.eu/en/press/press-releases/2019/10/07/better-protection-of-whistle-blowers-new-eu-wide-rules-to-kick-in-in-2021/.

4 "Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines", https://www.datenschutzkonferenz-online.de/media/oh/20181114_oh_whistleblowing_hotlines.pdf.