Baker McKenzie.

Hot Topics

Data & Technology
Germany

January 2020

The new EU Whistleblowing Directive: Considerations from a German compliance, employment and data protection law perspective

In December 2019, the Directive on the protection of persons who report breaches of Union law ("**Whistleblowing Directive**") entered into force[1]. Member States are required to transpose the Whistleblowing Directive into national laws ("**National Implementation Acts**") and to apply such National Implementation Acts as of 17 December 2021. The National Implementation Acts will have to require companies with more than 50 employees to implement internal compliance reporting channels[2] and to provide protection for certain whistleblowers (i.e., protection against retaliation).

Companies already having an internal whistleblowing system may need to make changes to such system depending on how anonymous reporting is handled, on permissible subject matters and on internal responsibilities. Details will, however, depend on the respective National Implementation Acts.

1. Key Provisions of the Whistleblowing Directive

The primary purpose of the Whistleblowing Directive is to protect whistleblowers who reported certain breaches of EU law[3] via the internal or external reporting channels provided by the Whistleblowing Directive in good faith.

- **Which companies are in scope?** Companies located in the EU with 50 or more employees will be required to implement an internal reporting system for certain compliance concerns. Furthermore, all companies, irrespective of the size, are required to ensure that whistleblowers are protected against any form of retaliating measures.
- **What protection shall be granted to whistleblowers?** As stated before, it is the Whistleblowing Directive's primary objective to have Member States protect whistleblowers who submitted a good-faith report in accordance with the National Implementation Acts. Companies will be required to refrain from any form of actual, threatened or attempted work-related retaliation against the whistleblower. The National Implementation

Our Expertise
Compliance & Investigations
Data & Technology
Employment & Compensation

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L1937&from=EN
[2] For companies with less than 250 employees, the obligation to establish such an internal reporting system does not apply until December 17, 2023.
[3] This includes EU regulations and directives as well as their national implementation laws in the field of public procurement, financial services, product and markets, prevention of money laundering and terrorist financing, product safety and compliance, transport safety, protection of the environment, radiation protection and nuclear safety, food and feed safety, animal health and welfare, public health, consumer protection or protection of privacy and personal data, and security of network and information system.

Acts 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.

Protection shall be granted (1) if 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 National Implementation Act and (2) if the whistleblower used the reporting channels foreseen by the Whistleblowing Directive. Furthermore, third parties who are connected to the whistleblower such as the whistleblower's colleagues or relatives shall also be protected provided they could also suffer work-related retaliation.

- **What types of subject matters are covered by the protection?** The Whistleblowing Directive provides an Annex which sets out certain EU laws relating to which a whistleblower may report a breach while being protected by the National Implementation Act. The Annex includes EU regulations and directives, including the national laws implementing those directives, in the field of public procurement, financial services, product and markets, prevention of money laundering and terrorist financing, product safety and compliance, transport safety, protection of the environment, radiation protection and nuclear safety, food and feed safety, animal health and welfare, public health, consumer protection or protection of privacy and personal data, and security of network and information system. The Whistleblowing Directive also protects whistleblowers reporting breaches affecting the financial interest of the EU and breaches relating to the internal market, including breaches of EU competition law, State aid rules, or corporate tax law.

  As of now, European Data Protection Authorities have taken the position that whistleblowing systems must be restricted to certain permissible subject matters. For example, the German Data Protection Authorities have reconfirmed in January 2019 (see our Client Alert) 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. Given the Whistleblowing Directive, those restrictions established by the data protection authorities may no longer apply in the future.

- **What will a reporting system look like?** National Implementation Acts will have to require companies to establish a reporting and investigation system having the following key features:

  - A company will be required to make the reporting system available to all employees.
  - The reporting system may also be made available to self-employed persons, trainees, applicants, shareholders as well as contractors, subcontractors and suppliers. In the latter case, the protection for whistleblowers will also extend to those whistleblowers.

- The reporting system can be operated internally by an individual or a company department, or externally by a service provider appointed by the company.
- The reporting system must be designed, established and operated in a secure manner that ensures the confidentiality of the whistleblower and any third party mentioned in the report. In addition, unauthorized employees must not have access to the reporting system.
- The internal reporting system must enable reporting in writing (for example by postal mail, by physical complaint boxes, or through an online platform) and/or orally (telephone or through other voice messaging systems). A whistleblower has also the right to request an in-person meeting to submit a report.
- In general, companies are obliged to acknowledge receipt of a report within seven days of receipt and to respond and follow-up to the whistleblower's report within three months after the acknowledgment.

▪ **To whom can a whistleblower make a report?** The Whistleblowing Directive recommends a 3-step reporting channel:

(1) Whistleblowers are encouraged to report a breach to the company via internal channels first ("internal reporting").

(2) Whistleblowers may make a report to the law enforcement agency or competent authority ("external reporting") following an internal reporting or directly without prior internal reporting.

(3) If the law enforcement agency or competent authority does also not take sufficient measures, the whistleblower may turn to the public ("public disclosures").

If the whistleblower wants to inform the public, the Whistleblowing Directive establishes certain requirements for the whistleblower to be protected, such as, the whistleblower must have reasonable grounds to believe (i) that the breach may constitute an imminent or manifest danger to the public interest, such as an emergency situation or a risk of irreversible damage; or (ii) that there is a risk of retaliation or a low likelihood of the breach being effectively addressed in case of external reporting (e.g., because evidence may be concealed or destroyed or an authority may be in collusion with the perpetrator of the breach or involved in the breach).

2. Aspects to be governed by Member States

The Whistleblowing Directive permits Member States to determine certain aspects by their national laws and as a consequence, different reporting systems may be necessary in the different Member States. For example, Member States can decide whether anonymous reporting shall be permitted, whether the permissible subject matters shall be expanded, and whether the rights of the whistleblowers shall be even more favourable than those of the Whistleblowing Directive. Sanctions for non-compliance may also vary in the National Implementation Acts.

3. German employment law considerations

From a German employment law perspective, the following is particularly noteworthy:

- **The protection awarded to whistleblowers is comprehensive**
  - The Whistleblowing Directive contains a **broad definition** of what actions (if in response to whistleblowing) qualify as retaliation, including, for example, the termination of employment, demotion, the decision not to extend a fixed-term contract and the blacklisting of employees within the relevant industry or sector (see 1. above for further examples).
  - Whistleblowers are **protected against potential claims** for breach of secrecy and other obligations not to disclose information provided they had reasonable grounds to believe that blowing the whistle was necessary for revealing a breach pursuant to the National Implementation Act.
  - Whistleblowers are entitled to remedies and compensation for any damage caused by retaliation in accordance with national law.
  - Whistleblowers are relieved from the burden of proving a link between their whistleblowing and an allegedly retaliatory action, which is one of the major shortcomings of existing whistleblowing protection laws (as in Germany, for example, where the burden of proving such link is on the employee). The Whistleblowing Directive shifts this burden to employers who will need to prove that their actions were based on duly justified grounds.
- **Rights and remedies cannot be waived or limited**
  - Rights and remedies provided for under the Whistleblowing Directive and, eventually, in the National Implementation Acts cannot be waived or limited by way of agreement, condition of employment or policy.
- **The Whistleblowing Directive does not affect the rights of social partners**
  - National laws providing for the right to information, consultation and participation as well as the employees' rights to consult with same remain unaffected.
  - With respect to internal reporting channels, the Whistleblowing Directive expressly refers to the rights of social partners to be consulted on and be sought to agree on the proposed establishment of such channels.

4. Effects on the legal assessment of the German Data Protection Authorities

Pursuant to the Whistleblowing Directive, the requirements of the GDPR remain unaffected. However, it is unclear how the requirements of the GDPR will be aligned with the protection granted under the Whistleblowing Directive. The German Data Protection Authorities, for example, determined that an individual who is mentioned in a whistleblowing report (in particular, the accused person) has the right to receive information about the identity of the whistleblower. Such an information disclosure will contradict with the confidentiality obligation under the

Whistleblowing Directive and, eventually, the National Implementation Act. We, therefore, expect that companies will be able to implement more comprehensive internal reporting systems in the future and build on being able to keep the identity of good faith reports confidential.

Katja Häferer
katja.haeferer
@bakermckenzie.com

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

Kerstin Grimhardt
kerstin.grimhardt
@bakermckenzie.com

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

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

Dr. Michaela Nebel
michaela.nebel
@bakermckenzie.com

Florian Tannen
florian.tannen
@bakermckenzie.com

Baker & McKenzie - Partnerschaft von Rechtsanwälten 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

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

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

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

www.bakermckenzie.com

Get Connected: