

FCPA Update

A Global Anti-Corruption Newsletter



Also in this issue:

7 Germany Enacts
Whistleblower Protection Act

[Click here for an index of
all FCPA Update articles](#)

If there are additional
individuals within
your organization who
would like to receive
FCPA Update, please email
prohlik@debevoise.com,
eogrosz@debevoise.com, or
pferenz@debevoise.com

FCPA Case Yields SEC's Largest-Ever Whistleblower Award

In May 2023, the SEC announced its largest-ever whistleblower award.¹ The nearly \$279 million payout rewarded a whistleblower's voluntary provision of information that helped support a successful FCPA enforcement action, and it more than doubled the SEC's previous record payout of \$114 million in 2020. In accord with whistleblower protection rules, the SEC did not disclose the whistleblower's identity, but press reported that the award was tied to telecom company Ericsson's \$1.06 billion FCPA settlements with the SEC and DOJ in 2019.²

[Continued on page 2](#)

1. U.S. Sec. & Exch. Comm'n Press Release No. 2023-89, "SEC Issues Largest-Ever Whistleblower Award" (May 5, 2023), <https://www.sec.gov/news/press-release/2023-89> ["May 2023 SEC Whistleblower Press Release"]; Order Determining Whistleblower Award Claims, Securities Exchange Act Release No. 97438 (May 5, 2023), <https://www.sec.gov/rules/other/2023/34-97438.pdf> ["May 2023 Whistleblower Order"].
2. Mengqi Sun, "Record \$279 Million Whistleblower Award Went to a Tipster on Ericsson," Wall St. J. (May 26, 2023), <https://www.wsj.com/articles/record-279-million-whistleblower-award-went-to-a-tipster-on-ericsson-5af40b98>.

**FCPA Case Yields
SEC's Largest-Ever
Whistleblower Award**

Continued from page 1

In a year during which there has been significant coverage of DOJ's recently enhanced incentives for companies to proactively invest in compliance programs, to voluntarily disclose wrongdoing, and to cooperate and remediate during government investigations,³ the SEC, through this whistleblower award announcement, is sending a loud message to employees to come forward with information about potential securities law violations. And while FCPA-related tips comprise only a small percentage of the total tips the SEC receives annually, this award announcement further demonstrates the outsized impact FCPA resolutions can have on companies and serves as a reminder to companies about the benefits of upfront investment in compliance and the need for robust internal controls.

SEC Whistleblower Program

The SEC's Whistleblower Program was created by the 2010 Dodd-Frank Act, which authorizes the SEC to provide monetary rewards to individuals who voluntarily provide the SEC original, timely, and credible information that leads to successful enforcement actions in which sanctions exceed \$1 million.⁴ Awards range between 10% and 30% of the amount collected and are paid out of an investor protection fund financed entirely through monetary sanctions paid to the SEC. The SEC whistleblower program also offers confidentiality protections and broadly protects whistleblowers from retaliation.

Whistleblower tips have contributed to enforcement actions resulting in orders requiring more than \$4 billion in disgorgement and interest.⁵ After a record year for whistleblower activity in FY 2021, in FY 2022, the SEC issued slightly fewer awards (103 versus 108) and for a smaller sum (\$229 million versus \$564 million), but received a record number of tips (12,322).⁶

The number of FCPA-related tips has remained largely consistent at approximately 200 per year over the past five years despite the large increase in the total number of tips in 2021 and 2022 (as shown below), but the FCPA-related tips appear to be yielding significant results.⁷ In addition to this largest-ever award (larger than the

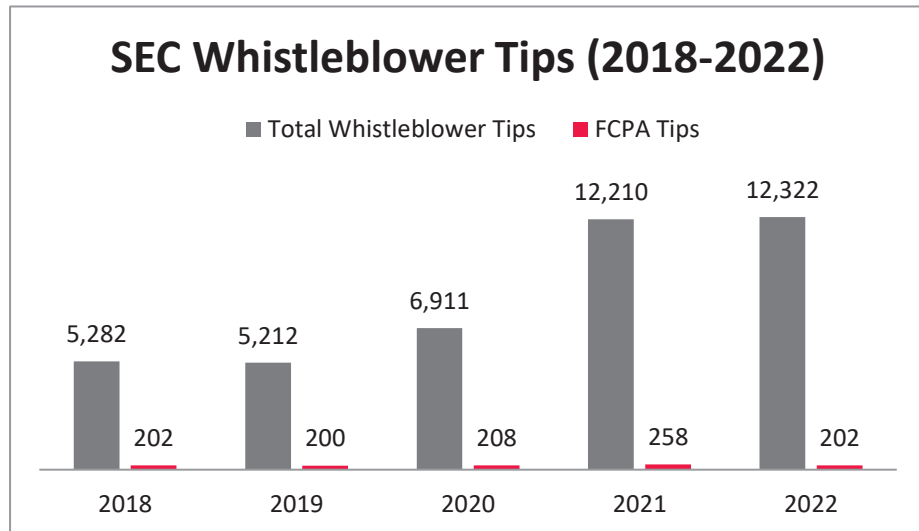
Continued on page 3

-
3. See, e.g., Debevoise in Depth, "DOJ Issues Trio of Updates that Further Heighten Compliance Expectations, Particularly Involving Off-System Communications and Compensation Systems" (Mar. 6, 2023), <https://www.debevoise.com/insights/publications/2023/03/doj-issues-trio-of-updates-that-further-heighten>; Debevoise Update, "DOJ Offers New Incentives in Revised Corporate Enforcement Policy" (Jan. 24, 2023), <https://www.debevoise.com/insights/publications/2023/01/doj-offers-new-incentives-in-revised>.
 4. See Winston M. Paes, Bruce E. Yannett, Philip Rohlik, & Taylor Booth, "SEC Pays \$28 Million in FCPA Whistleblower Award," FCPA Update, Vol. 12, No. 10 (May 2021), <https://www.debevoise.com/insights/publications/2021/05/fcpa-update-may-2021>.
 5. May 2023 SEC Whistleblower Press Release.
 6. Kara Brockmeyer et al., "The Year 2022 in Review: Normalcy Returns as Regulatory Expectations Rise," FCPA Update, Vol. 14, No. 6 (Jan. 2023), <https://www.debevoise.com/insights/publications/2023/01/fcpa-update-january-2023> ["Jan. 2023 FCPA Update"].
 7. *Id.*; see also Kara Brockmeyer et al., "SEC Enforcement Division's Year End Results Provide Insight into Record Breaking Year and Evolving Enforcement Agenda," FCPA Update, Vol. 14, No. 4 (Nov. 2022), <https://www.debevoise.com/insights/publications/2022/11/fcpa-update-november-2022>.

**FCPA Case Yields
SEC's Largest-Ever
Whistleblower Award**

Continued from page 2

previous three awards combined⁸), at least one 2022 award was reportedly tied to an FCPA resolution – a \$37 million award from an SEC settlement with a European healthcare company, which was the largest award that year.⁹



“[T]he SEC, through this whistleblower award announcement, is sending a loud message to employees to come forward with information about potential securities law violations.”

The Whistleblower(s)

According to press reports, the \$279 million tip provided SEC staff with information regarding conduct underlying parallel resolutions Ericsson reached in 2019 with the SEC and DOJ. According to the 2019 settlement papers, the company allegedly conspired to pay and improperly record bribes to foreign government officials in several countries in order to secure contracts from state-owned telecom companies over a 17-year period.¹⁰ The charges against Ericsson stemmed from alleged

Continued on page 4

8. U.S. Sec. & Exch. Comm’n, “Largest Whistleblower Awards” (June 4, 2022), <https://www.sec.gov/page/whistleblower-100million>.
 9. Mengqi Sun, “Whistleblower in Healthcare Bribery Case Won the Largest SEC Award This Year,” Wall St. J. (Dec. 19, 2022), <https://www.wsj.com/articles/whistleblower-in-healthcare-bribery-case-won-the-largest-sec-award-this-year-11671498462>.
 10. U.S. Sec. & Exch. Comm’n Press Release No. 2019-254, “SEC Charges Multinational Telecommunications Company with FCPA Violations” (Dec. 6, 2019), <https://www.sec.gov/news/press-release/2019-254>; U.S. Dep’t of Justice Press Release No. 19-1360, “Ericsson Agrees to Pay Over \$1 Billion to Resolve FCPA Case” (Dec. 6, 2019), <https://www.justice.gov/opa/pr/ericsson-agrees-pay-over-1-billion-resolve-fcpa-case>.

**FCPA Case Yields
SEC's Largest-Ever
Whistleblower Award**

Continued from page 3

activities in China, Djibouti, Indonesia, Kuwait, Saudi Arabia, and Vietnam between 2000 and 2017 that netted approximately \$427 million in profits. Ericsson agreed to pay approximately \$1.06 billion to resolve the charges – a \$520 million criminal penalty pursuant to a DPA with DOJ and disgorgement and prejudgment interest of \$540 million to the SEC. An Ericsson subsidiary also pleaded guilty to conspiracy to violate the FCPA's anti-bribery provisions, and Ericsson agreed to the appointment of an independent compliance monitor for a three-year period.

The SEC seeks tips that are timely, reliable, and specific, including by pointing to non-public content identifying a particular scheme, culpable individuals, and examples of witnessed wrongdoing.¹¹ In this matter, the whistleblower voluntarily provided original information that caused SEC staff (though the investigation had already been opened) to expand the scope of the investigation into wrongdoing that involved several countries over many years, which “saved the Commission significant time and resources.”¹² The whistleblower also provided “substantial, ongoing assistance” through multiple interviews and written submissions.

Two other individuals provided information to the SEC and applied to receive a whistleblower award in connection with the same matter, but their claims were denied because their information was either unrelated to the investigation and conduct charged or did not impact or advance the investigation.¹³ One of the denied whistleblowers, for example, claimed that the information they provided to the SEC partially motivated the SEC's decision to convert the case from a matter under inquiry to an investigation, but the SEC called that speculation and said the information had no bearing on opening the investigation. Both denied whistleblowers are appealing the SEC's denial, but rejections are seldom reversed.¹⁴

Whistleblower Tips and Takeaways

Headline-catching whistleblower rewards are likely to increase the numbers of tips, both from concerned compliance champions and less virtuous, opportunistic employees. (Indeed, even culpable individuals can be eligible for a whistleblower award.) It is important for companies to think about whistleblowers and their potential concerns both before and after they blow the whistle. Below are a few best practices and takeaways that companies should consider to mitigate whistleblower-related risks:

Continued on page 5

-
11. U.S. Sec. & Exch. Comm'n, Office of the Whistleblower, “Frequently Asked Questions” (Apr. 6, 2023), <https://www.sec.gov/whistleblower/frequently-asked-questions>.
 12. May 2023 Whistleblower Order at 5-6.
 13. *Id.* at 7-11.
 14. Mengqi Sun, “Other Tipsters Appeal After SEC Awarded One Whistleblower \$279 Million in Ericsson Case,” *Wall St. J.* (June 2, 2023), <https://www.wsj.com/articles/other-tipsters-appeal-after-sec-awarded-one-whistleblower-279-million-in-ericsson-case-c00a9984?page=1>.

FCPA Case Yields
SEC's Largest-Ever
Whistleblower Award

Continued from page 4

- **Think about whistleblowers before they blow the whistle and prioritize corporate compliance programs.** Companies should proactively invest in programs that ensure that compliance is incentivized and rewarded and that non-compliance is discouraged and sanctioned. This reduces risk and encourages a compliance-promoting culture in which employee concerns are invited, aired, and addressed without fear of retaliation and before escalation outside the company becomes necessary. Upfront investment also helps ensure that companies are prepared to respond appropriately when issues do arise.
 - *Policies and procedures:* Periodically review and evaluate policies and procedures related to complaint-handling processes and non-retaliation to ensure that they adequately address issues that arise from corruption and other relevant issues. Companies should also confirm that separation and other employment agreements comply with SEC Rule 21F-17, which requires that they not include language that impedes current or former employees from bringing information to the SEC about potential securities law violations. If applicable, policies and procedures should also now be adapted to account for increased remote work. After review, implement and follow these policies and procedures and ensure that employees know where to find them.
 - *Training:* Companies should train and remind employees and management – to whom whistleblower-related policies should be made available and easily accessible – about how to report and receive potential compliance complaints (e.g., reports to managers, anonymous reporting lines) and that non-retaliation is critical. Train or refresh relevant management regarding how to address complaints and how to minimize retaliation risk.
 - *Compliance resources:* Companies should ensure that they have legal and compliance teams with necessary qualifications and expertise, independence, and authority to execute internal review procedures, including by evaluating, triaging, and investigating the issues or allegations raised in employee reports. Take care not to involve persons potentially implicated by the allegations.
- **Address all complaints promptly and thoroughly.** Promptly, professionally, and thoroughly responding to employee complaints increases the likelihood of addressing concerns and avoiding escalation to the board, the SEC, social media, or the press. Not all reports will turn out to be credible; whistleblower complaints can be vague, perplexing, even inflammatory, and may appear to be opportunistic, but it is important to consider and take steps to address all concerns both individually and collectively. Whistleblowers often only have a partial view of the company's risks and are making complaints based on

Continued on page 6

FCPA Case Yields
SEC's Largest-Ever
Whistleblower Award

Continued from page 5

incomplete information, but there can be significant repercussions if legitimate concerns are dismissed wholesale because of their circumstances, including by whom or when they were raised.¹⁵

- **Do not interfere with the whistle being blown, or any time thereafter.** Section 21F of the Dodd-Frank Act and Exchange Act Rule 21F-17 prohibit impeding any person from contacting the SEC about a possible violation, including by threatening to enforce a confidentiality agreement.¹⁶ After a complaint comes in or the whistle has been blown, do not try to figure out the identity of an anonymous reporter or whistleblower, and if known, do not share the identity unless necessary for purposes of investigating raised concerns. Even the appearance of retaliation should be avoided. And this applies even when termination decisions are independently being contemplated for an employee with unsatisfactory performance, but who also happens to be raising concerns. Layoffs and employment decisions can lead to more employee complaints, and some employees could attempt to protect themselves from layoffs or express their dissatisfaction thereafter by making whistleblower complaints prior to or after termination. Legal and compliance personnel should collaborate with HR colleagues to thoroughly investigate and address all raised issues.
- **Consider consulting counsel.** To bolster privilege claims and provide a level of independence, consider engaging outside counsel when you receive complaints regarding alleged violations of law in connection with anti-corruption issues, particularly if any adverse action is being contemplated against the individual who has raised the concern.

Winston M. Paes

Andreas A. Glimenakis

Winston M. Paes is a partner in the New York office. Andreas A. Glimenakis is an associate in the Washington, D.C. office. Jacquelyn Sherman, a summer associate in the Washington, D.C. office, assisted in the preparation of this article. Full contact details for each author are available at www.debevoise.com.

Continued on page 7

15. See Debevoise Update, "Cybersecurity and AI Whistleblowers: Unique Challenges and Strategies for Reducing Risk" (Nov. 2, 2021), <https://www.debevoise.com/insights/publications/2021/11/cybersecurity-and-ai-whistleblowers>.

16. For example, last year the SEC charged The Brink's Company for using confidentiality agreements that prohibited disclosing without prior approval confidential information outside the company because there was no carveout for protected whistleblower contacts. Debevoise Update, "SEC Continues Focus on Lack of Whistleblower Carve Outs in Company Confidentiality Agreements" (June 30, 2022), <https://www.debevoise.com/insights/publications/2022/06/sec-continues-focus-on-lack-of-whistleblower>.

Germany Enacts Whistleblower Protection Act

On July 2, 2023, the German Whistleblower Protection Act¹ (*Hinweisgeberschutzgesetz*, “WPA”) enters into force. The WPA transposes the EU Whistleblower Directive (“Directive”) that protects reporting of certain work-related EU law violations.² The WPA exceeds the minimum requirements of the Directive by further protecting the reporting of work-related German criminal law and certain administrative law violations. The WPA protects the identity of a good faith whistleblower as well as the persons named in the whistleblower’s report, if the breaches are reported either internally within the organization or externally to dedicated government agencies, or publicly disclosed. Companies with more than 50 employees in Germany are now required to establish and maintain internal reporting channels and follow up on reports. While a good faith whistleblower is protected from retaliation, liability attaches to grossly negligent or intentionally false reporting. Violations of core WPA duties are sanctioned as administrative offences.

1. Background and Scope

Background

Until the enactment of the WPA, Germany has offered only fragmented whistleblower protection in instances such as reporting misconduct of companies under the supervision of the Federal Financial Supervisory Authority (*Bundesanstalt für Finanzdienstleistungsaufsicht*) or reporting violations of the Money Laundering Act (*Geldwäschegesetz*). Instead, whistleblower protection has been shaped by case law guided by the European Court of Human Rights (ECHR). In particular, the 2011 ECHR decision *Heinisch v. Germany*³ confirmed that whistleblowers must report internally first before reporting to authorities, and gave several criteria for permissible external reporting. In practice, however, the legal uncertainties in the case law presented considerable risk for whistleblowers.

The German legislature, when implementing the Directive, introduced clearer and more comprehensive protections for whistleblowers. The WPA does not replace, but rather supplements, already existing whistleblower protection rules.

Continued on page 8

-
1. Act for a better protection of whistleblowers and for the implementation of the Directive on the protection of persons who report breaches of Union law (*Gesetz für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden*), German Federal Law Gazette 2023 I no. 140, accessible here.
 2. Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law, OJL 305, 26.11.2019, p. 17–56, as amended, accessible here. See also Debevoise & Plimpton LLP, “EU Adopts Common Minimum Standards for Whistle-Blower Protection” (July 3, 2019), <https://www.debevoise.com/insights/publications/2019/07/eu-adopts-common-minimum-standards-for>.
 3. European Court of Human Rights, *Heinisch v. Germany* - 28274/08, Judgment 21 July 2011, accessible here.

Germany Enacts
Whistleblower Protection Act
Continued from page 7

Protected Persons

The WPA protects individuals who either report or publicly disclose breaches of certain laws on the basis of information acquired in a work-related context.

The protected individuals include current and former workers, civil servants, self-employed persons, volunteers, or trainees. The WPA further protects shareholders, persons in management, and persons working under the supervision and direction of contractors, subcontractors, and suppliers. The WPA protects not only the whistleblower, but also persons subject to the report or disclosure, and persons otherwise affected by the whistleblowing.

Protected Information

Reporting of information is protected if the information is obtained in connection with the whistleblower's professional activities and pertains to one of the enumerated laws listed in the WPA. Those laws include all criminal laws, as well as administrative offences to the extent they are protecting life, limb, and health, or protecting the rights of employees or employee representative bodies, such as a Works Council. Further, the protected information includes certain EU laws, as implemented, in fields such as money laundering, consumer rights, data protection, cybersecurity, financial audits, and competition.

There is no protection for reporting or publicly disclosing information relating to national security, or information covered by legal or medical professional secrecy. The professional secrecy of tax advisors or auditors, however, does not prevent whistleblower protection. If the information is a trade secret protected by the Trade Secrets Act (*Gesetz zum Schutz von Geschäftsgeheimnissen*), the reporting or public disclosure is permitted if the reporting person has reasonable grounds to believe that the sharing or disclosure is required to detect a breach. The same rule applies if the information is protected by a contractual duty of confidentiality, e.g., a non-disclosure agreement in an employment contract.

2. Reporting

In General

The WPA protects a whistleblower who reports in one of three permitted ways: internally through employer reporting channels, externally to government authorities, or – in rare instances – through public disclosure.

The whistleblower may now choose freely between internal or external reporting. The WPA encourages the whistleblower to report internally if the violation can be addressed effectively and the reporting person believes that there is no risk of retaliation. Employers are encouraged to incentivize internal reporting.

Continued on page 9

**Germany Enacts
Whistleblower Protection Act**
Continued from page 8

The internal or external reporting offices are bound to ensure during all stages of the investigation the confidentiality of the identities of the reporting person, persons subject to the reporting, and persons otherwise affected by the whistleblowing. The duty to protect those identities also applies vis-à-vis the company's management.

The confidentiality of the whistleblower's identity is not protected if they did not have reasonable grounds to believe that the reported information is within the scope of the WPA, or if they intentionally or with gross negligence reported false information. There is also no protection of the whistleblower's identity when complying with a request from authorities in the context of criminal or administrative proceedings, or a court decision. Furthermore, the whistleblower's identity is not protected to the extent that sharing of the information is necessary for follow-up measures or the sharing is based on the consent of the whistleblower. However, an employee's consent must meet the strict data protection requirements of being freely given. Finally, the identity of the person subject to the report may be shared for purposes of internal investigations.

“The German legislature, when implementing the Directive, introduced clearer and more comprehensive protections for whistleblowers. The WPA does not replace, but rather supplements, already existing whistleblower protection rules.”

The whistleblower report is documented and must be retained, at a minimum, for three years after the closing of the investigation, unless a further retention is provided for by law, and is necessary and proportionate.

Internal Reporting

Every employer employing regularly 50 or more employees in Germany is obliged to establish channels and procedures for internal reporting, and for follow-up. A grace period until December 17, 2023 applies if the number of employees is less than 250. However, there is neither a minimum employee number nor a grace period for employers in the financial industry, including investment services firms, banks, and asset management companies.

Continued on page 10

Germany Enacts
Whistleblower Protection Act
Continued from page 9

Each employer must grant the internal reporting office the powers necessary to carry out its tasks. The office may be operated internally by a person or department designated for that purpose or externally by a third party. Employers in the private sector with regularly 50 to 249 workers may share resources regarding the receipt of reports and any investigation to be carried out. According to the explanatory notes to the WPA and in response to a different view of the EU Commission, centralized reporting channels in a group are permissible. Neither the use of a third party nor the sharing of resources prejudices the obligations of the employer to address the reported breach. The WPA requires the persons tasked with the internal reporting office to be independent and skilled. Unless there is a conflict of interest, the person also may conduct other activities for the employer.

The internal channels for reporting must accept reporting in writing or orally, either by telephone or another voice messaging system, or by means of a physical meeting within a reasonable timeframe. The channels for receiving the reports must be designed, established, and operated in a secure manner that ensures that only authorized persons have access to the reports.

After a long debate regarding the permissibility of anonymous reporting, the legislature decided that the internal reporting office must process anonymous reports, if received. There is, however, no duty to design internal reporting channels in a way that permits the submission of anonymous reports.

The internal reporting office must provide acknowledgement of receipt of the report to the reporting person within seven days; it must check if the report is within the scope of WPA and relevant; and it is obliged to maintain communication with the reporting person and take follow-up measures such as conducting an internal investigation or referring the reporting person to the authorities. It generally must give feedback to the reporting person within three months, informing them about planned or taken measures while protecting the identity of the persons involved.

The establishment of an internal reporting office and its policies and procedures touch on the competence of the Works Council that must be involved. With a view to the use of personal data for processing whistleblower reports, the Data Protection Officer also must be consulted.

External Reporting

Whistleblowers that choose to report externally can turn to the centralized external reporting office with the Federal Office of Justice (*Bundesamt der Justiz*). The Federal Financial Supervisory Authority (*Bundesamt für Finanzdienstleistungsaufsicht*) and the Federal Cartel Office (*Bundeskartellamt*) serve within their respective competence as further external reporting offices.

Continued on page 11

Germany Enacts
Whistleblower Protection Act
Continued from page 10

The external reporting offices establish reporting channels, check the relevance of the reports, and take follow-up measures in proceedings similar to the internal reporting offices of employers.

3. Public Disclosure

Whistleblowers who publicly disclose alleged violations are protected only in two limited circumstances: *first*, if - following external reporting - no appropriate action was taken or they received no information on appropriate action within the statutory timeframes; and *second*, if the whistleblower has reasonable grounds to believe that the breach may constitute an imminent or manifest danger to the public interest, or, in the case of external reporting, there is a risk of retaliation or a low prospect of the breach being effectively addressed.

4. Whistleblower Protection

A prerequisite for the protection of the whistleblower under the WPA is, *first*, the use of an appropriate reporting channel or public disclosure; *second*, reasonable grounds to believe that the information was true; and *third*, reasonable grounds to believe that the information is within the scope of the WPA. The protection extends to individuals supporting the whistleblower confidentially, as well as third parties suffering retaliation.

The whistleblower shall not incur criminal, administrative, or civil liability in respect of acquiring or accessing the reported or disclosed information. If, however, the acquisition or access to the information constitutes, as such, a crime, the reporting person will not benefit from immunity. There is no violation of confidentiality duties if the whistleblower has reasonable grounds to believe that the information-sharing was required to detect a violation.

The WPA prohibits any form of retaliation, including threats or attempted retaliation. The WPA lists a wide variety of possible detrimental measures that includes dismissal, disciplinary measures, and discrimination, but also early termination and cancellation of a contract for goods and services. In proceedings before a court or an authority relating to a disadvantage suffered by the whistleblower, it is presumed that the detriment resulted from retaliation for the report or disclosure if the whistleblower so alleges. The burden of proof shifts to the person who took the detrimental measure, in many cases the employer, to show that the measure was based on sufficient grounds or was not caused by the reporting or disclosure. A thorough documentation of the reasoning for measures taken can assist this rebuttal.

A whistleblower who suffers retaliation is further entitled to compensation for pecuniary damages.

Continued on page 12

Germany Enacts
Whistleblower Protection Act
Continued from page 11

The whistleblower is, however, liable for any damage caused by an intentionally or grossly negligent reporting or public disclosure of false information.

Contractual restrictions of the rights of whistleblowers or other persons protected under the WPA, e.g. in employment agreements, are void.

5. Data Protection

The use of personal information for whistleblowing triggers the EU General Data Protection Regulation (GDPR) and the Federal Data Protection Act (*Bundesdatenschutzgesetz*). The WPA is the legal basis for the processing of personal data by internal and external reporting offices and permits, subject to the implementation of precautions, the use of sensitive data without consent.

The WPA has no specific rules on how to balance whistleblower confidentiality with data protection transparency if, for example, a reported person seeks information about the whistleblower's identity via a GDPR data subject access request. In this case, the employer must strike a balance between the whistleblower interests protected by the WPA and the GDPR on the one hand, and the rights of the accused person on the other hand, including the right to defend their case in a fair trial.

6. Administrative Penalties

The public disclosure of wrong information is an administrative offence if the disclosing person knows that the information is wrong. It is also an administrative offense if a person hinders reporting, does not implement or maintain an internal reporting system, takes retaliatory measures, or does not preserve the confidentiality of the protected persons. The administrative fine can be up to EUR 50,000, and in certain instances for corporations up to EUR 500,000.

7. Conclusion

While there is general consensus in Germany that a whistleblower system is a key element of sound corporate governance, in practice only large corporations already have such systems in place.

The WPA has the potential to change business culture in several respects. *First*, the legislature now has acknowledged the value of the contribution of whistleblowers to the detection and punishment of misconduct by introducing a more comprehensive system of whistleblower protection. *Second*, the new freedom of the whistleblower to effectively choose between internal and external reporting channels incentivizes companies to make internal reporting more attractive, so that

Continued on page 13

**Germany Enacts
Whistleblower Protection Act**
Continued from page 12

they will learn of potential wrongdoing prior to the authorities. *Third*, the WPA expressly does not address the rules of criminal procedure, including the power of the public prosecutor to seize whistleblower reports stored in the internal reporting office for the mandatory retention period. This might be another incentive for companies to properly investigate alleged misconduct to reduce or avoid their own corporate criminal or civil liability.

Companies operating in Germany will have to check their existing whistleblowing systems against the WPA requirements and, if operating also in other EU Member States, consider that the implementation of the Directive elsewhere in the EU may differ from the WPA.⁴

Karolos Seeger

Friedrich Popp

Karolos Seeger is a partner in the London office. Friedrich Popp is an international counsel in the Frankfurt office. Full contact details for each author are available at www.debevoise.com.

4. See, e.g., Debevoise & Plimpton LLP, "France Beefs Up Whistleblower Protections" (Mar. 23, 2022), <https://www.debevoise.com/insights/publications/2022/03/france-beefs-up-whistleblower-protections>.

FCPA Update

FCPA Update is a publication of
Debevoise & Plimpton LLP

66 Hudson Boulevard
New York, New York 10001
+1 212 909 6000
www.debevoise.com

Washington, D.C.
+1 202 383 8000

San Francisco
+1 415 738 5700

London
+44 20 7786 9000

Paris
+33 1 40 73 12 12

Frankfurt
+49 69 2097 5000

Hong Kong
+852 2160 9800

Shanghai
+86 21 5047 1800

Luxembourg
+352 27 33 54 00

Bruce E. Yannett
Co-Editor-in-Chief
+1 212 909 6495
beyannett@debevoise.com

Andrew J. Ceresney
Co-Editor-in-Chief
+1 212 909 6947
aceresney@debevoise.com

David A. O'Neil
Co-Editor-in-Chief
+1 202 383 8040
daoneil@debevoise.com

Karolos Seeger
Co-Editor-in-Chief
+44 20 7786 9042
kseeger@debevoise.com

Douglas S. Zolkind
Co-Editor-in-Chief
+1 212 909 6804
dzolkind@debevoise.com

Philip Rohlik
Co-Executive Editor
+852 2160 9856
prohlik@debevoise.com

Kara Brockmeyer
Co-Editor-in-Chief
+1 202 383 8120
kbrockmeyer@debevoise.com

Andrew M. Levine
Co-Editor-in-Chief
+1 212 909 6069
amlevine@debevoise.com

Winston M. Paes
Co-Editor-in-Chief
+1 212 909 6896
wmpaes@debevoise.com

Jane Shvets
Co-Editor-in-Chief
+44 20 7786 9163
jshvets@debevoise.com

Erich O. Grosz
Co-Executive Editor
+1 212 909 6808
eogrosz@debevoise.com

Andreas A. Glimenakis
Associate Editor
+1 202 383 8138
aaglimen@debevoise.com

Please address inquiries regarding topics covered in this publication to the editors.

All content © 2023 Debevoise & Plimpton LLP. All rights reserved. The articles appearing in this publication provide summary information only and are not intended as legal advice. Readers should seek specific legal advice before taking any action with respect to the matters discussed herein. Any discussion of U.S. Federal tax law contained in these articles was not intended or written to be used, and it cannot be used by any taxpayer, for the purpose of avoiding penalties that may be imposed on the taxpayer under U.S. Federal tax law.

Please note:
The URLs in *FCPA Update* are provided with hyperlinks so as to enable readers to gain easy access to cited materials.