AN A.S. PRATT PUBLICATION
FEBRUARY-MARCH 2020
VOL. 6 • NO. 2

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 6 | NUMBER 2 | FEBRUARY/MARCH 2020

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [6] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [33] (LexisNexis A.S. Pratt)

An A.S. Pratt™ Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2020–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquiries and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report,* LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

EU Adopts Whistleblowing Directive to Protect Whistleblowers

By Alja Poler De Zwart*

The new Directive on the protection of persons who report breaches of European Union law, also referred to as the "Whistleblowing Directive," will require Member States to create rules that mandate organizations with more than 50 workers to set up whistleblowing hotlines and accept reports about violations of the EU law. This article provides an overview of the main requirements and takeaways of the Whistleblowing Directive.

Whistleblowing rules in Europe are about to change dramatically. The new directive on the protection of persons who report breaches of Union law,[1] also referred to as the "Whistleblowing Directive," will require Member States to create rules that mandate organizations with more than 50 workers to set up whistleblowing hotlines and accept reports about violations of the EU law.

The Whistleblowing Directive also provides for minimum standards on how to respond to and handle concerns raised by whistleblowers. These minimum requirements provide sufficient details so that organizations can start reviewing their existing whistleblowing hotlines (if they already have them in place) and adjusting their internal processes to align with the Whistleblowing Directive.

This article provides an overview of the main requirements and takeaways of the Whistleblowing Directive.

WHICH ORGANIZATIONS WILL NEED TO COMPLY?

The Whistleblowing Directive requires organizations with more than 50 "workers" to set up reporting channels. This is a big change compared to the current situation, where the majority of Member States do not legally require the establishment of such reporting channels.

The concept of a "worker" in the EU is broad and, according to settled EU case-law, covers persons who, for a certain period of time, perform services for and under the direction of another person, in return for which they receive remuneration. This includes not only regular employees but also workers in non-standard employment relationships, including part-time workers, trainees/interns, and fixed-term contract workers. This may be problematic for certain organizations whose numbers of

* Alja Poler De Zwart is a partner at Morrison & Foerster LLP, representing clients in privacy and data protection matters. She may be contacted at apolerdezwart@mofo.com.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:PE_78_2019_REV_1&from=EN.

"workers" fluctuate around the 50 mark. If your organization is not certain whether it hits the 50 mark, or it does sometimes but not always, it might be prudent to take a "better safe than sorry" approach and set up the channels anyway.

The Whistleblowing Directive furthermore gives Member States the right to "encourage" organizations in private sectors with fewer than 50 workers to also establish internal reporting channels. If a Member State chooses to do so, it can impose less prescriptive requirements for such channels then currently laid down in the Whistleblowing Directive, provided that such requirements guarantee confidentiality and diligent follow-up. This is something to keep and mind and see what such "encouragements" will look like.

The Whistleblowing Directive does not specify whether the 50 workers need to be physically located in the EU. A reasonable interpretation is that any legal entity established in the EU that employs more than 50 workers will need to comply with the Whistleblowing Directive, no matter if such workers are located in or outside the EU. It is unclear whether non-EU entities that employ more than 50 workers who are located in the EU will need to comply with the Whistleblowing Directive.

However, it is highly likely that such entities will be subject to the Whistleblowing Directive, considering that European labor law, including regulations on worker protection and other employee protection provisions, applies to employees located in the EU, regardless of their employer's seat. EU Member States' implementing laws will hopefully provide additional clarity on this point.

WHAT WILL BE THE ALLOWED SCOPE OF THE WHISTLEBLOWING REPORTS?

Unlike the current rules where the scope of the hotlines is generally quite narrow and varies per EU Member State, the whistleblowers will now be allowed to report, at a minimum, about a broad range of violations of the EU law including:

- Public procurement;
- Financial services, products and markets, and prevention of money laundering and terrorist financing;
- Product safety;
- Transport safety;
- Protection of the environment;
- Radiation protection and nuclear safety;
- Food safety, animal health and welfare;
- Public health;

- Consumer protection;
- Protection of privacy and personal data, and security of network and information systems;
- Violations affecting the financial interests of the EU; and
- Violations relating to the internal market, including violation of EU competition and State aid rules, and corporate tax law.

Note that Member States may extend the scope of reportable concerns when they implement the Whistleblowing Directive into their national law. The expectation is that some Member States might indeed take advantage of this option. This might, for example, be the case for the Netherlands, where the current House for Whistleblowers Act already requires organizations with at least 50 workers to allow for reporting of "suspicious wrongdoing" without limiting such wrongdoing to violations of the EU law.

IS THERE A PRESCRIBED FORM FOR THE REPORTING MECHANISM?

The Whistleblowing Directive requires organizations to enable individuals to report in:

- Writing and submit reports by post, by physical complaint box(es), or through an online platform (via the internet or an internet platform); and/or
- To report orally, by telephone hotline, or other voice messaging system.

Note that upon whistleblower's request, such channels should also enable reporting by means of physical meetings, within a reasonable timeframe.

Third parties may also be engaged to receive reports on behalf of the organization, provided such third parties offer appropriate guarantees for independence, confidentiality, data protection, and secrecy. The Whistleblowing Directive suggests that such third parties could be external reporting platform providers, external counsel, auditors, trade union representatives, or employees' representatives.

WHO WILL BE PROTECTED BY THE WHISTLEBLOWING DIRECTIVE?

The Whistleblowing Directive offers protection to whistleblowers who have acquired information on violations of the EU law in a "work-based relationship." This protection will be granted to the broadest possible range of categories of individuals, irrespective of whether they are EU citizens or third-country nationals, the nature of their activities, or whether they are paid. This includes:

- Individuals having the status of workers, such as current and former (part- or full-time) employees and temporary workers;

- Individuals who are not workers but can play a key role in exposing violations of the EU law and may find themselves in a position of economic vulnerability in the context of their work-related activities, such as self-employed providing services, freelance workers, contractors, subcontractors, suppliers, shareholders, and persons in managerial bodies;
- Job applicants or individuals seeking to provide services to an organization, who (i) acquire relevant information during the recruitment process or another pre-contractual negotiation stage, and (ii) could suffer retaliation (e.g., in the form of negative employment references, blacklisting, or business boycotting); and
- Volunteers and paid, or unpaid, trainees.

WHAT TYPE OF PROTECTION WILL BE OFFERED TO WHISTLEBLOWERS?

The Whistleblowing Directive requires Member States to prohibit any form of retaliation. If whistleblowers do suffer retaliation, the Whistleblowing Directive requires the Member States to set up the following protective measures:

- *Advice*: Whistleblowers will be provided with free of charge access to comprehensive and independent information and advice on available procedures and remedies;
- *Remedial measures*: Whistleblowers will be provided with appropriate remedial measures against retaliation, including:
    - Interim relief to (i) halt ongoing workplace retaliation (such as threats or harassment), or (ii) prevent dismissal pending the resolution of legal proceedings;
    - Reversal of the burden of proof, requiring organizations to prove that they are not retaliating against the whistleblower;
- *Protection from liability*: Whistleblowers will not be considered to have breached any restriction on disclosure of information imposed by contract or law (e.g., "gagging" clauses) and will not incur liability for making whistleblowing disclosures;
- *Protection in judicial proceedings*: In legal proceedings, whistleblowers will be able to rely on the Whistleblowing Directive and its implementing laws for the purpose of their defense; and
- *Other measures*: Such as financial assistance and psychological support.

The Whistleblowing Directive also suggests that a clear legal prohibition of retaliation has an important dissuasive effect and would be further strengthened by provisions for personal liability and penalties for the perpetrators of retaliation.

WHEN WILL THE PROTECTION APPLY?

In order to be protected under the Whistleblowing Directive, the whistleblower needs to only have reasonable grounds to believe (in light of the circumstances and the information available to them at the time of reporting) that the concern reported is true. The motives of the whistleblowers are irrelevant in deciding whether they should receive protection.

IS ANONYMOUS REPORTING ALLOWED?

The Whistleblowing Directive notes that it does not affect the power of Member States to decide whether organizations and competent authorities are required to accept and follow up on anonymous reports. Thus, this issue is left to the Member States to decide in their national implementation. The Whistleblowing Directive, however, also notes that whistleblowers who reported or publicly disclosed information on violations of the EU law anonymously, but are subsequently identified and suffer retaliation, will still qualify for the Whistleblowing Directive's protection.

HOW SHOULD THE REPORTS BE HANDLED BY ORGANIZATIONS?

These are the key obligations that organizations need to consider:

- *Information about the reporting process*: Organizations need to provide sufficient information about the internal reporting process as well as the procedures on how they can report externally (to competent authorities; see next question below). Such information could be posted at a visible location that is easily accessible to all potential whistleblowers (such as company website);
- *Confidentiality*: Reporting channels must be designed and operated in a secure manner that ensures confidentiality of the identity of the (i) whistleblower, (ii) any facilitators (meaning individuals who assist the whistleblower in the reporting process), as well as (iii) third parties mentioned in the report;
- *Impartiality*: Organizations must designate impartial person or department to investigate reports independently and free of conflict of interest (e.g., dual function held by a company officer well placed to report directly to the organizational head, such as a chief compliance or human resources officer, an integrity officer, a legal or privacy officer, a chief financial officer, a chief audit executive, or a member of the board);
- *Diligent investigation*: Organizations must ensure diligent investigation of the reported concerns;
- *Asking for clarifications*: Organizations may ask for further information during the course of the investigation, but without obligating the whistleblower to do so;

- *Acknowledgement*: Organizations must acknowledge receipt of a report unless the whistleblower explicitly requested otherwise;
- *Feedback & timelines*: Organizations must provide feedback to the whistleblower within three months. The timeframe can be extended to six months in duly justified cases (e.g., when the nature and complexity of the report requires a lengthy investigation). The feedback should include:
    - The action envisaged or taken following the report; and
    - The grounds for the choice of that action.

The whistleblower does not need to receive this feedback as long as providing it could prejudice the investigation or affect the rights of the implicated individuals. Where the appropriate action still needs to be determined, the whistleblower also needs to be informed accordingly. Note that in all cases, the whistleblower should be informed of the investigation's progress and outcome.

DOES THE WHISTLEBLOWER HAVE TO REPORT CONCERNS TO INTERNAL WHISTLEBLOWING HOTLINE?

The Whistleblowing Directive notes that whistleblowers should be encouraged to first use internal reporting channels and report to their organization, if such channels are available to them and can reasonably be expected to work. If this is not the case, whistleblowers may:

- *Report concerns to competent Member State/EU authorities*: The authorities are also required to establish appropriate external reporting channels, to diligently follow up on the reports received, and, within a reasonable timeframe, give feedback to whistleblowers. The whistleblowers have the right to report their concerns directly to such authorities where:
    - Organizations did not set up internal channels, or internal channels were used but did not function properly (e.g., because the report was not dealt with diligently or within a reasonable timeframe, or no appropriate action was taken despite the internal investigation confirming the existence of a breach); or
    - A whistleblower has valid reasons to believe that: (i) he/she would suffer retaliation; or (ii) the competent authorities would be better placed to take effective action. The latter would, for example, be the case where:
        (i) The ultimate responsibility holder within the work-related context is involved in the breach;

(ii) There is a risk that the breach or related evidence could be concealed or destroyed;

(iii) The effectiveness of investigative actions by competent authorities might be jeopardized (e.g., in the case of cartel and other violations of competition rules); or

(iv) The breach requires urgent action (e.g., to safeguard the health and safety of persons or to protect the environment); and

- *Make public disclosures*: The whistleblower may make a public disclosure if, despite making a report internally and/or externally, the breach remains unaddressed. This can be the case, for example, if the reported breach was not appropriately investigated, no appropriate remedial action was taken, there is a risk of retaliation, or there is a low prospect of the breach being effectively addressed due to the particular circumstances of the case (e.g., evidence could be concealed or destroyed, or an authority might be in collusion with the perpetrator of the breach or even involved in the breach).

WHAT CAN YOUR ORGANIZATION DO NOW?

The Member States will need to implement the Whistleblowing Directive into local law over the course of the next two years. Organizations with 250 or more workers will therefore need to comply with the new rules by December 17, 2021, while the organizations with 50 to 249 workers have an additional two years to become compliant (December 17, 2023). National implementation inevitably means that there will be no full harmonization, so the whistleblowing rules in the EU will likely remain segmented per country. This is, to a certain extent, bad news for multinational organizations that have operations in various EU Member States. Over the next two years, organizations should continue monitoring the Member States' implementation to identify specific local deviations and thereupon adjust their hotlines accordingly.

Considering that the minimum standards are set by the Whistleblowing Directive, organizations might already consider taking the following steps:

- If your organization does not have a whistleblowing hotline yet, then this is the time to start setting one up. The process of setting up such reporting channels is usually not as simple as it looks, and it often includes engagement of a third-party whistleblowing hotline provider that can facilitate an online and phone line reporting process. So the sooner your organization starts preparing, the better.

- If your organization already has a whistleblowing hotline in place, then it can review the workings of the hotline and adjust the relevant internal processes to what the Whistleblowing Directive already requires. This could, for example, include:

    - Adjusting the scope of concerns allowed to be reported in the EU to violations of the EU law, unless the current scope in a specific Member State (such as in the Netherlands) is already broader than this;
    - If the whistleblowing hotline is currently available only to your organization's current personnel, opening the hotline externally for other individuals such as former employees, job applicants, individuals seeking to provide services, subcontractors, suppliers, volunteers, trainees, and business partners;
    - Adjusting the processes to enable reporting by means of physical meetings with the whistleblowers that can be set up within a reasonable timeframe;
    - Checking and ensuring that a person or a department that is designated to investigate the whistleblowing reports can indeed do so in an independent and impartial manner, free of conflict;
    - Ensuring that the whistleblowers are not pressured to provide additional information when requested by the designated investigators. This will likely include instructing and training the investigators on (i) how to ask for such input to ensure maximum response; and (ii) knowing when to stop if the whistleblower does not want to cooperate anymore. Internal investigation protocols that provide uniform instructions on what investigators may and may not do are, as always, highly recommended;
    - Providing sufficient information to potential whistleblowers about the internal reporting process, as well as the procedures on how they can report externally, by means of an updated whistleblowing policy or notice;
    - Setting up a process to (i) acknowledge receipt of a report unless the whistleblower explicitly requests otherwise, and (ii) providing feedback within the abovementioned timelines;
    - In light of the possibility of whistleblowers reporting their concerns to external channels, setting up effective and independent processes for whistleblowers to complain about not being taken seriously, or being subject of retaliation; and
    - Consider what else can be done to make individuals feel comfortable reporting internally. For example, consider ensuring that the reporting channels are:

        (i) Available 24/7;

        (ii) Are simple and easy to use;

(iii) Offer anonymity (where allowed on Member State law level);

(iv) Are available in local languages;

(v) Provide transparent explanatory information and simple instructions; and

(vi) Are accompanied by an effective internal communication and investigation strategy.

Also, consider making it very clear within the organization that retaliation is absolutely prohibited, and individuals disregarding this prohibition in any way or form will be subject to severe disciplinary measures, including termination of employment.