ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Whistleblowing in the European Union

Technology, Privacy, and eCommerce

Whistleblowing, where a person with knowledge can report behaviors that are allegedly illegal, is a concept that is recognized globally, albeit with varying degrees of legitimacy or protection. In October 2019, the European Union passed its Whistleblowing Directive. Member states have two years to enact appropriate national laws.

Prior to the enactment of the EU Whistleblowing Directive, there were only 10 countries in the European Union with whistleblower protection laws. The variation in these respective whistleblowing laws drove the need for the unifying directive.

The EU directive prohibits retaliation against whistleblowers and applies to any employers that have more than 50 employees. It encourages employers to develop internal whistleblowing mechanisms, which can be anything as simple as a box to submit paper complaints or as sophisticated as an online mechanism run by third parties. The directive contemplates that not all whistleblowers will feel comfortable reporting internally, and if the reporter feels there is a threat then he or she is able to report the behavior publicly, including through social media.

Those seeking to be compliant with the EU Whistleblowers Directive should also be aware of how it considers data privacy and interacts with existing privacy regulations.

The European Union’s approach is that whistleblowers should only report on breaches of European law. This includes such topics as financial services, public safety and compliance, transport safety, protection of the environment, food and feed safety, animal health and welfare, consumer protection, public health, protection of privacy and personal data, and security of network and information systems. Other behavior, such as sexual harassment at work, may very well not fall within the laws addressed by the EU directive. Employers may need to develop a plan to manage complaints about misbehaviors that are not subject to the EU Whistleblowing Directive.

Question of anonymity

The General Data Protection Regulation (GDPR) offers a complexity to whistleblowing on both the reporting side as well as the investigation side. For employers to avoid the complications of data processing consent (and potential subsequent revocation of consent) for the person who is blowing the whistle, employers might recommend anonymous reporting. But this also brings in the complication of needing enough detail in order to substantiate and investigate the complaint. Historically, the European Union has not supported traditional anonymous whistleblowing hotlines. Much of this stemmed from the requirement that individuals who are being accused of misbehavior have the right to know who is reporting them. This tension between the reporter and the accused remains but is recognized.

The individual who is the subject of the complaint has the right to know about the data being processed and may object to the processing. An employer could cite legitimate interest or substantiation of legal claims as its legal basis depending on the nature of the complaint but must conduct a data protection impact assessment on the process of whistleblowing investigations.

Maintaining personal data

There is also the added complication of the requirement to only maintain personal data for the time period pertinent to that data. Like the data processing, this is a complexity mainly under GDPR, but it is a significant enough complexity to warrant its own itemization. When it comes to legal investigations, retention may be an extended period of time. Here again, we see the challenge of following data protection requirements in the realm of a litigious society.

It is not illogical to maintain whistleblower complaints for years in anticipation of litigation or to track a pattern of behavior. However, the European Union expects findings to be communicated back to the reporter no later than three months, and if the accused individual is cleared, the records should be destroyed. If the alleged behavior is substantiated, the investigation should move to action taken to address the issue and once addressed, destroy the records.

Companies operating in the European Union will face challenges, but not insurmountable ones. It will take diligence on the side of legal and compliance to build and implement a functional, substantial, and compliant whistleblowing program

Please see the text of the EU Directive 2019/1937

K Royal

Associate General Counsel

TrustArc

Reach out to K about her column at @heartofprivacy on Twitter, or www.linkedin.com/in/kroyal/.