Editorial

Tilmann Dittrich

Article - Version of Record

International Cybersecurity Law Review (2023) 4:255–258
https://doi.org/10.1365/s43439-023-00096-9

EDITORIAL

Editorial

Tilmann Dittrich

Accepted: 26 June 2023 / Published online: 13 July 2023

1 IT security helps compliance monitors cross the pond

The use of compliance monitors has so far been met with reluctance in Germany. They are well known in the United States, where compliance monitors are deployed on the orders of authorities when companies have become conspicuous due to compliance incidents. In addition to possible sanctions, it can be ensured over a defined period of time that companies change their compliance management system after an incident in order to avoid similar errors in the future, as this is an elementary component of a compliance management system.

A first comprehensive attempt to establish such monitoring structures in Germany was made by the draft Association Sanctions Act (VerSanG) published in 2020. As is well known, it did not become law, but due to a recent decision at the Conference of Ministers of Justice in May 2023 in Berlin to encourage the Federal Minister of Justice to resubmit such a draft law, discussions will continue in this regard. Section 13 (2) of the draft VerSanG provided that the court may order an association to take certain precautions after a compliance incident in order to avoid further incidents and to prove these precautions by certification of a competent body—ergo a compliance monitor.

The German NIS-2 Implementation and Cybersecurity Strengthening Act (NIS2UmsuCG) will lead the way by bringing the instrument of compliance monitors to the German legal system, but the act covers only IT security cases. This law implements the new European NIS-2 Directive for cybersecurity. An estimated 30,000 additional companies and public institutions will be subject to this completely revamped German Act on the Federal Office for Information Security (BSIG) in the future, which will be changed by NIS2UmsuCG. In order to

✉ Tilmann Dittrich
Heinrich-Heine-Universität Düsseldorf, Düsseldorf, Germany
E-Mail: tilmannd@googlemail.com

implement Article 32 (4) (g) of the NIS-2 Directive, Section 64 (5) of the draft NIS2UmsuCG stipulates that the Federal Office for Information Security can designate a monitoring officer for essential entities and other critical infrastructure tasked with overseeing the cybersecurity risk management requirements and the reporting obligations in the event of security incidents. This monitor is appointed for a fixed time period and with a precisely defined scope of their task.

To date it has not been agreed upon as to who is best suited to perform the duties of a monitoring officer. The draft VerSanG mentioned auditors, lawyers, and management consultants as examples. In any case, sound IT security knowledge from a legal perspective, as well as awareness of management processes and the technical background, will be required for this assignment. The author believes, therefore, that it would be prudent to further define the professional and personal qualifications required in a law or act and to create a mandatory certification from the BSI. It remains to be seen whether the entities, as previously stipulated in the German draft of the VerSanG, will have the right to recommend or at least have a say in the appointment of such a monitor by the authorities. Hopefully, the future will see the BSI use the instrument of compliance monitors regularly to assess compliance incidents, thereby reducing financial sanctions and at the same time introducing improvements to the whole cybersecurity compliance, which is an essential part of a compliance monitoring system.

2 Die IT-Sicherheit verhilft dem Compliance Monitorship über den großen Teich

Der Einsatz von Compliance Monitors ist in Deutschland bislang auf Zurückhaltung gestoßen. Das Modell stammt aus den USA, wo Behörden Compliance Monitors in Unternehmen einsetzen können, die durch Compliance-Vorfälle auffällig geworden sind. Zusätzlich zu einer etwaigen Sanktion kann so über einen definierten Zeitraum sichergestellt werden, dass Unternehmen ihr Compliance-Management-System nach einem Vorfall anpassen, um so zukünftig gleichförmige Fehler zu vermeiden. Diese vorfallsbedingte Systemverbesserung ist elementarer Bestandteil eines Compliance-Management-Systems.

Einen ersten umfassenden Anlauf zur Etablierung solcher Monitoring-Strukturen in Deutschland unternahm der 2020 veröffentlichte Entwurf für ein *Gesetz zur Stärkung der Wirtschaft*, kurz *Verbandssanktionengesetz* (VerSanG). Der Entwurf wurde bekanntlich zwar nicht Gesetz, aber aufgrund eines jüngsten Beschlusses auf der Justizministerkonferenz im Mai 2023 in Berlin, der den Bundesjustizminister zur erneuten Vorlage eines solchen Gesetzentwurfs bewegen will, werden diesbezüglich die Diskussionen weiter fortschreiten. § 13 Abs. 2 VerSanG-E sah vor, dass das Gericht einen Verband nach einer Verbandstat – wenn folglich eine Straftat begangen wurde – durch die Pflichten, die den Verband betreffen, verletzt wurden, anweisen kann, bestimmte Vorkehrungen zur Vermeidung von Verbandstaten zu treffen und diese Vorkehrungen durch Bescheinigung einer *sachkundigen Stelle* – ergo eines Compliance Monitors – nachzuweisen.

Doch bevor mit dem VerSanG eine solche allgemeine Möglichkeit zum Einsatz eines Compliance Monitors geschaffen werden konnte, schreiten entsprechende Entwicklungen im IT-Sicherheitsrecht schneller voran. Grund hierfür ist das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG), das die NIS-2-RL in Deutschland umsetzt. Mit diesem künftigen Gesetz werden geschätzt 30.000 zusätzliche Unternehmen und öffentliche Einrichtungen einem umfassend veränderten BSIG mit weitreichenden Compliance-Pflichten zur IT-Sicherheit unterliegen. Zur Umsetzung von Art. 32 Abs. 4 lit. g NIS-2-RL sieht der Entwurf in § 64 Abs. 5 NIS2UmsuCG vor, dass das Bundesamt für Sicherheit in der Informationstechnik für die besonders wichtigen Einrichtungen sowie kritischen Anlagen zur Überwachung der Vorgaben zum Cybersicherheits-Risikomanagement sowie zu den Meldepflichten bei Sicherheitsvorfällen einen *Überwachungsbeauftragten* für einen definierten Zeitraum unter Festlegung eines genauen Aufgabenspektrums benennen kann.

Bislang ist noch unklar, wer zur Ausübung des Amts dieses Überwachungsbeauftragten am geeignetsten erscheint. Der VerSanG-E nannte beispielhaft Wirtschaftsprüfer, Rechtsanwälte sowie Unternehmensberatungen. Der Schwerpunkt der Tätigkeiten eines Überwachungsbeauftragten i. S. d. BSIG aber liegt in der Überwachung der technischen Einhaltung von Rechtsvorschriften. Erforderlich sind daher fundierte IT-Sicherheitskenntnisse aus rechtlicher Sicht. Ergänzende Grundkenntnisse über die technischen Zusammenhänge sowie in den Unternehmen etablierte Management-Prozesse sind ebenfalls unerlässlich. Aus Sicht des Verfassers ist es daher sinnvoll, die fachlichen und persönlichen Voraussetzungen per Gesetz oder Verordnung näher festzulegen und an eine Zertifizierung beim BSI anzuknüpfen. Spannend dürfte in Zukunft auch sein, ob den Unternehmen und Einrichtungen, wie etwa im VerSanG-E vorgesehen, ein Vorschlagsrecht, zumindest aber ein Mitspracherecht für die Person des Compliance-Monitors von Behördenseite aus eingeräumt wird. Insgesamt bleibt zu hoffen, dass das BSI das Instrument des Überwachungsbeauftragten in Zukunft regelmäßig bei der Bewertung von Rechtsverstößen heranziehen wird, da so Bußgeldsanktionen abgesenkt werden können und gleichzeitig die systemverbessernde Wirkung der IT-Sicherheit eintreten kann, auf die gerade die Bußgeldsanktionen ebenfalls abzielen.

Funding Open Access funding enabled and organized by Projekt DEAL.

Tilmann Dittrich LL.M. (Medizinrecht), Law clerk in the area of the Düsseldorf Higher Regional Court and PhD student at Heinrich-Heine-University Düsseldorf