Das Magazin für Führungskräfte in Kirchen und kirchlichen Organisationen

www.kviid.de

KVI im DIALOG

4 | November 2022

Finanzen
Grundlagen des Rechnungswesens von kirchlichen, caritativen und diakonischen Vereinen - Kostenrechnung, Planung und Budgetierung als Teile des Reportings, Teil 9

Recht und Steuern
Hinweisgeber-Systeme und deren datenschutzrechtlichen Relevanzen

KVI Kongress 2022 Special
Der KVI Kongress 2022 verbuchte einen neuen Rekord - Das digitale Kongressformat hat sich erneut bewährt

Energie und Umwelt
EKD-Klimaschutzrichtlinie - Ein Meilenstein auf dem Weg zur Klimaneutralität

Informationstechnologien
AWO und ihr Weg in die Cloud - Bezirksverband Baden geht mit der Cloud in eine digitale Zukunft

Personalmanagement
Du kannst auch warten, bis es kracht - Wie Konflikte nicht nur gelöst, sondern auch zur Weiterentwicklung genutzt werden können

Digital.Durchdacht. Durchstarten

Digitale Instrumente zur Personalgewinnung, -bindung und -qualifizierung

HINWEISGEBER

Hinweisgeber-Systeme und deren datenschutzrechtliche Relevanzen

Ein Beitrag von Dr. Nico Herold und Johannes Norpoth

Im Anschluss an sein Studium hat Dr. Nico Herold zu den Themen Compliance, Korruption und Whistleblowing geforscht - insbesondere im Bereich des Gesundheitswesens. Als Rechtsanwalt und Manager ist er bei Curacon in der Beratung von Mandaten zu Compliance-/Hinweisgeber-Systemen tätig.

Johannes Norpoth ist Manager im Bereich Unternehmensberatung-Datenschutz von Curacon. Der diplomierte Sozialwissenschaftler hat über die zurückliegenden drei Jahrzehnte in unterschiedlichen Verantwortungspositionen in Einrichtungen des Gesundheits- und Sozialwesens gearbeitet.

Ende September hat der Deutsche Bundestag in der erster Lesung über den Regierungs-Entwurf eines Gesetzes für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden beraten (HinSchG-E).[1] Nachdem in der letzten Legislaturperiode die Umsetzung der europäischen Richtlinie zum Whistleblowing [(EU) 2019/1937 – WB-RL] in nationales Recht an den Differenzen zwischen den Koalitionspartnern gescheitert ist, dürfte im aktuellen Anlauf die Umsetzung gelingen.

Damit kommen voraussichtlich mit Inkrafttreten des HinSchG in erstem Quartal 2023 auf viele Unternehmen und Einrichtungen – auch aus dem Gesundheits- und Sozialwesen – erhebliche Anforderungen zu.

Von besonderer Bedeutung ist nicht nur eine gesetzeskonforme Umsetzung im betrieblichen Alltag. Der Hinweisgeberschutz ist immer auch im Kontext bestehender datenschutzrechtlicher Anforderungen zu sehen. Nach einem Überblick über den aktuellen Gesetzesentwurf erläutern die Autoren insbesondere den datenschutzrechtlichen Kontext und diesbezügliche Relevanzen für Hinweisgeber-Systeme.

Was ist Whistleblowing?

Unter Whistleblowing versteht man ganz allgemein die Weitergabe von Informationen über Missstände bzw. über Fehlverhalten in Organisationen. Die Weitergabe kann zum einen intern erfolgen, etwa gegenüber der Organisationsführung, dem Betriebsrat, internen Meldesystemen oder externen Dienstleistern im Sinne von Ombudsstellen. Externes Whistleblowing bezeichnet zum anderen die Weitergabe an die Kontroll- und Strafverfolgungsbehörden oder die Öffentlichkeit, meist in Form der Medien. [2]

Der HinSchG-E greift dieses Verständnis auf, differenziert aber die beiden externen Varianten und beschränkt die Adressaten interner und externen Meldungen auf die Meldestellen im Sinne des Gesetzes. Somit sind Meldungen Mitteilungen von Informationen über Verstöße an interne oder externe Meldestellen, während eine Offenlegung das Zugänglichmachen von Informationen über Verstöße gegenüber der Öffentlichkeit bezeichnet (§ 3 Abs. 4 und 5).

Dazu definiert § 1 Abs. 1 eine hinweisgebende Personen sehr weit als: natürliche Personen, die im Zusammenhang mit ihrer beruflichen Tätigkeit oder im Vorfeld einer beruflichen Tätigkeit Informationen über Verstöße erlangt haben und diese an die nach dem HinSchG-E vorgesehenen Meldestellen melden oder offenlegen.

Wozu dienen Whistleblowing und Hinweisgeber-Systeme?

Der Sinn und Zweck von Whistleblowing ist mehrdimensional: Für Organisationen dient Whistleblowing als eine Art „Frühwarnsystem von unten nach oben“: Insider melden frühzeitig Verstöße, die sonst nicht bekannt würden oder nicht zur Sprache kämen.

Damit soll die Selbst- und interne Sozialkontrolle verbessert und so externes Whistleblowing mit den

damit einhergehenden Haftungs- und Reputationsschäden für die Organisation vermieden werden.

Für die Strafverfolgungs- und Kontrollbehörden ergeben sich durch eingehende Hinweise Informations- und Verfolgungsansätze, die nur schwer mit den konventionellen Ermittlungsmethoden zu erreichen wären, z.B. im Feld der Korruption. Hinweisgeber-Systeme sollen meldewilligen Insidern attraktive und niedrigschwellige interne und externe Meldeumgebungen bieten – und damit auch zu einer Stimulierung und Kanalisierung von Hinweisen in die jeweiligen Kanäle führen.

Es entsteht damit ein Konkurrenzverhältnis um das Hinweisgeber-Wissen und die Erstverarbeitungshoheit zwischen internen und externen Adressaten.[3] Organisationen sollten das besonders vor den Neuerungen des HinSchG-E ernst nehmen.

Was dürfen Hinweisgeber zukünftig und welchen Schutz genießen sie?

Kernelement der Rechte von Hinweisgebern im Sinne des HinSchG-E und der WB-RL ist das neue Wahlrecht bei internen und externen Meldestellen.

Hinweisgeber werden sich aussuchen können, ob sie sich an die organisationseigene Meldestelle (dazu näher unten) wenden oder aber direkt die externe Meldestelle der Behörden informieren (§ 7 Abs. 1 HinSchG-E; Art. 10 WB-RL). Nur die Offenlegung ist erst nachrangig geregelt, etwa in Notfällen oder wenn nicht angemessen auf eine externe Meldung reagiert wird oder dann Repressalien zu befürchten sind (§ 32 HinSchG-E).

Dann werden nicht nur Sie als die hinweisgebende Person, sondern auch die bei der Meldung unterstützenden Personen sowie Dritte

Abb.: Colourbox

Unter Whistleblowing versteht man ganz allgemein die Weitergabe von Informationen über Missstände bzw. über Fehlverhalten in Organisationen.

und juristische Personen im Eigentum der hinweisgebenden Person geschützt (§ 33 HinSchG-E).

Der Schutz umfasst ungerechtfertigte Benachteiligungen aller Art, die im Zusammenhang mit einem bestehenden Dienst- oder Arbeitsverhältnis und eine Reaktion auf die Meldung/Offenlegung darstellen, wie z.B. eine Kündigung oder Mobbing (§§ 3 Abs. 6 und 36 HinSchG-E, Liste in Art. 19 WB-RL).

Zudem unterliegen auch die Beschaffung, der Zugriff auf und die Weitergabe der Information bei gutem Glauben an die Erforderlichkeit dem Schutz des Gesetzes, soweit die Beschaffung keine Strafgesetze verletzt (§ 35 Abs. 1).

Darüber hinaus führt der HinSchG-E weitere Schutzkomponenten ein, etwa eine Beweislastumkehr für die kausale Verknüpfung von Nachteilen und Meldung zur Repressalie, Vertraulichkeitsgebot, Ausschluss der Haftung/Verantwortlichkeit für rechtmäßige Meldungen/Offenlegungen und Schadensersatz für erlittene Repressalien (§§ 35 f.).

Wer muss was wie einrichten?

Grundsätzlich müssen alle juristischen Personen des privaten und öffentlichen Rechts mit mehr als 50 Beschäftigten (mindestens) eine interne Meldestelle einrichten (§ 12 Abs. 1 und 2 HinSchG-E). Dabei gilt für juristische Personen des privaten Sektors mit 50 bis 249 Beschäftigten die Gestaltungsoption, gemeinsame Meldestellen einzurichten oder sich entsprechende Ressourcen zu teilen (§ 14 Abs. 2 S. 1 HinSchG-E).

Für diese Unternehmensgruppe gilt auch eine Schonfrist bis zum 31.12.2023 (§ 42 HinSchG-E). Ausdrücklich gestattet ist auch die Betrauung von Dritten – etwa Rechtanwaltskanzleien – mit den Aufgaben der internen Meldestelle (§ 12 Abs. 1 S. 1 HinSchG-E).

… und was passiert wenn …

kein Hinweisgebersystem eingerichtet wird? Nach dem HinSchG-E kann ein Bußgeld von bis zu 20.000 Euro verhängt werden, wenn der Verpflichtung zur Einrichtung/Betrieb einer internen Meldestelle nicht nachgekommen wird.

RECHTLICHE

Wo tangiert ein Hinweisgebersystem den Datenschutz?

Insgesamt berühren Whistleblowing und die (zukünftig verpflichtende) Einrichtung und der Betrieb eines Hinweisgeber-Systems zahlreiche unterschiedliche Rechtsgebiete. Neben dem Arbeitsrecht, Strafrecht-/Ordnungswidrigkeitenrecht, dem jeweiligen Branchenrecht gilt das insbesondere für das Datenschutzrecht.[4]

Zulässigkeit der Datenverarbeitung

In Anwendungsbereich der DSGVO gilt immer das Verbot der Datenverarbeitung mit Erlaubnisvorbehalt (Art. 6 Abs. 1 DSGVO). Schon an diesem Grundprinzip zeigt sich, dass dem Datenschutzrecht eine hohe rechtliche Komplexität zugrunde liegt. Im Zusammenhang mit Hinweisgeber-Systemen sind insbesondere folgende datenschutzrechtlichen Fragen relevant: Zulässigkeit der Datenverarbeitung, Informations-/Unterrichtungs- und Aufklärungspflichten von Hinweisgeber und Betroffenen der Meldung, Dokumentations- und Löschpflichten sowie die Beteiligung von Datenschutzbeauftragten und entsprechende Folgenabschätzungen.

Die Erlaubnis ergibt sich für die Aufgaben einer Meldestelle zunächst aus der speziellen Zulässigkeitsnorm des § 10 HinSchG-E – grds. nur für Organisationen, die auch zur Einrichtung verpflichtet sind.

Parallele Zulässigkeiten ergeben sich aus dem allgemeinen Datenschutzrecht der DSGVO, ggf. in Verbindung mit dem Bundesdatenschutzgesetz (BDSG) oder etwa Spezialbereichen bei elektronischen Hinweisgeber-Systemen etwa aus dem Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG).

Abb.: Colourbox

Das bevorstehende Hinweisgeberschutzgesetz (HinSchG) bringt vielfältige Anforderungen mit sich.

Infrage kommt insbesondere die Erfüllung rechtlicher Pflichten gem. § 6 Abs. 1 c) DSGVO, die hier in der Einrichtung und dem Betrieb einer Meldestelle liegen (§§ 11 f. HinSchG-E). Die individuelle Einwilligung als Verarbeitungsbasis ist wenig geeignet, da sie neben dem Hinweisgeber auch von den von der Meldung betroffenen Personen abgegeben werden müsste, wofür diese nicht nur informiert sondern wozu sie auch bereit sein müssten. Außerdem kann sie jederzeit widerrufen werden (Art. 7 Abs. 3 S. 1 DSGVO).

Informations- und Aufklärungspflichten der Betroffenen

Dies betrifft im Kontext des Whistleblowings vor allem die von der Meldung betroffenen Personen. Es besteht eine Pflicht zu deren Information über die Verarbeitung der personenbezogenen Daten (Zweck, Art, Speicherung etc.) mit einer Maximal-Frist von einem Monat ab Erlangung der Daten (Art. 14 Abs. 3 DSGVO). Zusätzlich steht ihnen ein entsprechender Auskunftsanspruch zu (Art. 15 Abs. 1 DSGVO).

Daraus ergibt sich die zentrale Kollision zwischen HinSchG-E und dem Datenschutzrecht. Auf Seiten der Hinweisgeber-Systeme stehen die grundsätzliche Vertraulichkeit der Meldung (§ 8 HinSchG-E) und die wirksame Aufklärung des gemeldeten Verstoßes (§§ 16 f. HinSchG-E). Auf Seiten der von der Meldung betroffenen Personen steht das „Recht, zu wissen“.

Zugunsten der Bearbeitung der Meldung kann man sich hier auf verschiedene – teils komplizierte Ausnahmen – berufen. Exemplarisch genannt werden können hier Ausnahmen von der Informationspflicht, etwa ausdrückliche Regelung der widerstreitenden Interessen gemäß Art. 14 Abs. 5 c) DSGVO i.V.m. § 8 Abs. 1 Nr. 1 HinSchG-E (Vertraulichkeitsgebot der Identität) oder § 33 Abs. 1 Nr. 2 a) BDSG (Informationserteilung beeinträchtigt zivilrechtliche Ansprüche).

Dokumentations- und Löschpflichten

Aus dem Datenschutzrecht leitet sich auch das „Recht auf Vergessenwerden“ ab (Art. 17 Abs. 1

DSGVO). Die damit verbundenen Löschpflichten kollidieren mit der Dokumentationspflicht nach § 11 HinSchG-E. Demnach sind alle eingehenden Meldungen in dauerhaft abrufbarer Weise zu dokumentieren und zwei Jahre nach Abschluss des jeweiligen Bearbeitungs-Verfahrens zu löschen.

Aus dem allgemeinen Datenschutzrecht ergeben sich auch an dieser Stelle anderslautende Löschpflichten.

Beispielsweise sind personenbezogene Daten u.a. dann unverzüglich zu löschen, wenn keine Notwendigkeit für den Erhebungszweck mehr besteht [Art. 17 Abs. 1 a) DSGVO] – etwa zur Geltendmachung, Ausübung oder zur Verteidigung von laufenden oder wahrscheinlichen Rechtsansprüchen [Art. 17 Abs. 3 e) DSGVO] bzw. gem. § 24 Abs. 1 Nr. 2 BDSG für zivilrechtliche Ansprüche.

Die Datenschutzkonferenz (DSK) nennt eine allgemeine Löschfrist von zwei Monaten nach Abschluss der Untersuchung[5] und auch die WB-RL bestimmt, dass keine Aufbewahrung länger als erforderlich und verhältnismäßig sein darf, um die Anforderungen dieser Richtlinie zu erfüllen (Art. 18 Abs. 1). Es bleibt abzuwarten, wie sich dieses Spannungsverhältnis praktikabel auflösen lässt.

Beteiligung von Datenschutz und Datenschutz-Folgenabschätzung

Aus Art. 38 DSGVO leitet sich die unbedingte Zuziehung des Datenschutzbeauftragten bei der Implementierung eines Hinweisgeberschutzsystems in der eigenen Organisation ab.

Darüber hinaus ist grundsätzlich, aber insbesondere auch im Kontext der hier erläuterten widerstrebenden Interessen, eine Datenschutz-Folgenabschätzung zur Beschreibung der Verarbeitungsvorgänge und der daraus ableitbaren Risiken für die betroffenen Personen unumgänglich.

Sofern externe Dienstleister als Auftragsverarbeiter im Sinne des Art. 28 DSGVO zum Einsatz kommen, ist eine sorgfältige und umfassende Prüfung auf Basis des Art. 32 DSGVO vorzunehmen.

Fazit

Das bevorstehende HinSchG bringt vielfältige Anforderungen mit sich und das für den überwiegenden Teil von Unternehmen und Organisationen – auch im Bereich von Gesundheitswesen und der Sozialwirtschaft.

Neben diesen operativen Aufgaben steht der Hinweisgeberschutz in einem äußerst komplexen Verhältnis diverser Rechtsgebiete.

Schon allein die singuläre und ausschnittartige Betrachtung des Datenschutzes zur Gewährleistung und Sicherung der Interessen aller in einem Hinweisgeber-System agierenden und von einem solchen System betroffenen Akteure zeigt eine erhebliche und detailtiefe Komplexität. Mit steigender Komplexität steigt immer auch das Risiko, als Betreiber in haftungsrelevante Datenschutzverstöße zu geraten.

Das ist insbesondere besonders delikat, weil der HinSchG-E Datenschutzverstöße im sachlichen Anwendungsbereich erfasst und diese folglich über die Hinweisgeber-Systeme zulässigerweise und mit der damit verbundenen Schutzwirkung gemeldet werden können [§ 2 Abs. 1 Nr. 3 o) und p)].

Insofern sind jeder Verantwortliche für den Datenschutz, aber auch Datenschutzbeauftragte sehr gut beraten, vor einer Implementierung eines eigenen Hinweisgeber-System die eigenen Ressourcen ehrlich zu bewerten, um nicht später unkalkulierbaren Haftungsrisiken und Reputationsschäden aus dem Hinweisgeber-System selbst wie aus dem allgemeinen Datenschutz ausgesetzt zu sein.

Literaturhinweise

1. https://www.bundestag.de/dokumente/textarchiv/2022/kw39-de-hinweisgebende-personen-911404
2. Kölbel/Herold/Wienhausen-Knezevic (2022), Kapitel 1: Whistleblowing als Gegenstand der gesellschaftlichen Reflexion: Semantik und Konzeption, in: Kölbel (Hrsg.), Whistleblowing. Band 1: Stand und Perspektiven der empirischen Forschung, Heidelberg: C.F. Müller, S. 1 ff., 17 f.
3. Herold (2022), Kapitel 2: Whistleblowing als Individualphänomen: Faktoren und Prozesse der Mitteilungsentscheidung, in: Kölbel (Hrsg.), Whistleblowing. Band 1: Stand und Perspektiven der empirischen Forschung, Heidelberg: C.F. Müller, 51 ff. m.w.N.
4. Siehe für das Folgende Nickel, Compliance-Berater 1-2/2022, 20 ff.; Croonenbrock/Hansen (2022), Arbeitsrecht Aktuell 14 (6), 139 ff.; Altenbach/Dierkes (2020), Corporate Compliance Zeitschrift 13 (3), 126 ff.
5. DSK (2018), Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz, 10 ff.