Vertrauliche Meldewege: die Whistleblower-RL in der Praxis

Vortrag bei der Stiftung Datenschutz am 9.11.2021

RA Wolfgang Schmid

Ihr Referent: Wolfgang Schmid

- Wir sind
  - 5 Rechtsanwälte und Spezialisten für IT-Recht
  - 5 Externe Datenschutzbeauftragte, Datenschutzauditoren, seit 2004
  - Ombudsmann in Whistleblowing-Systemen seit 2011
  - Vorsitzender im FA-Ausschuss IT-Recht der RAK München, Referent der Deutschen Anwaltakademie

und heute glücklich, dass ich vor Ihnen referieren darf!

Telefon 0821 – 4540543, Mail wolfgang.schmid@schmid-frank.de

Die neue Whistleblowing Richtlinie

Hintergrund:

- Im Oktober 2019 hat die EU die „Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden“ verabschiedet
- Rechtslage in Europa bislang uneinheitlich, UK, Irland, Frankreich, Schweden schon viel weiter
- In Deutschland kein Hinweisgeberschutzgesetz

Die neue Whistleblowing Richtlinie

Wer ist betroffen?

- Unternehmen mit mehr als 50 Mitarbeitern, keine Übergangsregelung, aber gemeinsame Nutzung von Hinweisgebersystemen möglich
- Behörden und Kommunen ebenfalls ab 50 Mitarbeiter, leider auch ohne Übergangsregelung (z.B. Gemeinden mit weniger als 10.000 Einwohner)

Die neue Whistleblowing Richtlinie

Persönlicher Anwendungsbereich	Sachlicher Anwendungsbereich
• Geschützt werden sämtliche Personen im beruflichen Kontext, z.B. Arbeitnehmer, Bewerber im Rahmen des Bewerbungsverfahrens, Selbstständige, Anteilseigner, Praktikanten, Subunternehmer, Lieferanten • Geschützt werden darüber hinaus Dritte, die mit dem Hinweisgeber in Kontakt stehen und ebenfalls berufliche Repressalien erleiden könnten, z.B. Verwandte und Kollegen	• Verstoß (auch „missbräuchliche Handlungen“), auch wenn noch nicht eingetreten, aber mit hoher Wahrscheinlichkeit zu rechnen • Verstöße sind Handeln, Unterlassen, Versuche der Verschleierung • Begründete Bedenken ohne eindeutige Beweise • Der Schutz umfasst Meldungen von Verstößen gegen Unionsrecht im Bereich des Strafrecht, Ordnungswidrigkeitenrechts, Vergaberechts, Finanzdienstleistungen, Geldwäsche, Terrorismus, Produktsicherheit, Verkehrssicherheit, Umweltschutz, Verbraucherschutz, Schutz der Netzsysteme, Datenschutz, u.s.w.

Die neue Whistleblowing Richtlinie

Inhalte und Ziele:

- Europaweiter, einheitlicher Rechtsrahmen für den Schutz von Hinweisgebern
- Pflicht zur Einführung interner und externer Meldesysteme
- Hinweisgebern sollen bessere Möglichkeiten haben, Missstände zu melden
- Hinweisgeber sollen besser vor Repressalien geschützt werden

Hinweisgebersysteme

Technische Anforderungen nach der RL:

- Meldekanäle müssen so konzipiert sein, dass Unbefugte keinen Zugriff haben
- Identität des Hinweisgebers muss geschützt sein
- Meldekanäle müssen unabhängig und selbstständig organisiert sein

Hinweisgebersysteme

Internes Meldesystem	mit Hilfe Dritter
• Strenge Anforderungen • Unbefugte dürfen keinen Zugriff erhalten • Identität des Hinweisgebers und Dritter bleibt geschützt • Unternehmen muss dem Hinweisgeber innerhalb von 7 Tagen Eingang der Meldung bestätigen und innerhalb von 3 Monaten informieren, wie mit dem Hinweis umgegangen wurde und welche Maßnahmen ergriffen wurden	• Unternehmen müssen zuständige Dritten (Prüfer, Gewerkschaftsvertreter, Rechtsanwalt) benennen, der zur Entgegennahme der Meldung befugt ist • Unternehmen müssen diesen Dritten mit den entsprechenden Ressourcen hierfür ausstatten

Achtung Wording: Die „externe“ Meldung ist die Meldung an die Behörde

Hinweisgebersysteme

Meldekanäle (in Abgrenzung zu den Folgemaßnahmen mit Prüfung auf Stichhaltigkeit):

- Whistleblowing-Hotline, mündlich oder schriftlich
  - Hotline bietet direkten und persönlichen Kontakt zu Ombudsperson, Verschlüsselung in Mail-Kommunikation

- IT-gestützte Plattform
  - Kann durch den Betrieb selbst konfiguriert und programmiert werden oder von einem Drittanbieter genutzt werden
  - Online-Meldesystem mit verschlüsseltem Verfahren
  - Vorgefertigter Fragenkatalog kann die wesentlichen Aspekte bereits abklären und so den Hinweis bereits bei der Meldung kategorisieren, Probleme mit dem „scheuen Reh“?

Betriebsrat

- Strittig: betreffen Whistleblower-Regelungen das Ordnungsverhalten der Arbeitnehmer und sind daher gem. § 87 Abs. 1 Nr. 1 BetrVG mitbestimmungspflichtig?

- Ist das plattformgestützten Hinweisgebersystemen eine „technischen Einrichtung zum Zwecke der Verhaltens- oder Leistungsüberwachung“ des Arbeitnehmers im Sinne des § 87 Abs. 1 Nr. 6 BetrVG

Datenschutz und Hinweisgebersysteme

Personenbezogene Daten?

- Angaben über die beschuldigte Person und je nach Sachverhalt weitere betroffene Personen wie z. B. Zeuge oder Kollegen
- Sachverhalt des Verstoßes
- Wenn keine Anonymisierung des Hinweisgebers erfolgt, werden auch dessen Name und z. B. Position im Unternehmen sowie die Umstände der Beobachtung des Verstoßes verarbeitet

Datenschutz und Hinweisgebersysteme

Die Whistleblowing-RL enthält mehrere Regelungen in Bezug auf Datenschutz:

- EG 54, EG 74, EG 76

Datenschutz und Hinweisgebersysteme

- Art. 17, Verarbeitung personenbezogener Daten:

Die nach dieser Richtlinie vorgenommene Verarbeitung personenbezogener Daten ein-schließlich des Austauschs oder der Übermittlung personenbezogener Daten durch die zuständigen Behörden erfolgt im Einklang mit der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680. ..

Personenbezogene Daten, die für die Bearbeitung einer spezifischen Meldung offensichtlich nicht relevant sind, werden nicht erhoben bzw. unverzüglich wieder gelöscht, falls sie unbeabsichtigt erhoben wurden.

Datenschutz und Hinweisgebersysteme

Mittendrin…

- Im Hinweisgeberverfahren werden stets personenbezogene Daten übermittelt, in der Regel Beschäftigtendaten, also § 26 Abs. 1 S. 2 BDSG (zu dokumentierende Anhaltspunkte) iVm Art. 88 DSGVO (Verpfeifer und die Pfeife…);
  damit Anwendung sämtlicher Vorschriften der DSGVO über die Wertung des Art. 88 und § 26 Abs. 5 BDSG
- Einwilligung, § 26 Abs. 2 S. 1 BDSG nur bezogen auf Bekanntgabe Person des Hinweisgebers durch ihn selbst möglich

Datenschutz und Hinweisgebersysteme

statt nur dabei:

- Nach DSK 14112018 wohl Art. 6 I lit c. DSGVO, wegen rechtlicher Verpflichtung zur Korruptionsbekämpfung, nationales WB-Gesetz fehlt, auch Verbandssanktionengesetz ist gescheitert;
- nach DSK auch kein Art. 6 I lit b., da Beschäftigungsverhältnis nicht betroffen ???
- Wenn Legitimation über Art 6 I lit. f DSGVO, dann Problem der Verarbeitung „weicher Faktoren“ (Freundlichkeit, ethische Konformität)

Datenschutz und Hinweisgebersysteme

- Nachweis der Einhaltung aller Datenschutzprinzipien
- Datenschutzprinzipien sind
  - Rechtmäßigkeit und Transparenz der Verarbeitung, Art. 5 Abs. 1 lit. a DSGVO
  - Zweckbindung, Art. 5 Abs. 1 lit. b DSGVO
  - Datenminimierung Art. 5 lit. c DSGVO durch bestmögliche Pseudonymisierung, EG 78
  - Datenrichtigkeit, Art. 5 Abs. 1 lit. d DSGVO
  - Speicherbegrenzung, Art. 5 Abs. 1 lit. e DSGVO
  - Integrität Art. 5 Abs. 1 lit. f DSGVO (TOMs)
- Datenschutzfolgenabschätzung

Datenschutz und Hinweisgebersysteme

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen – wie z. B. Pseudonymisierung –, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen. (bekannt auch Art. 25 I DSGVO)

Datenschutz und Hinweisgebersysteme

- Zweckbindung zur Missbrauchsvorbeugung
  - Um einen Missbrauch des Meldekanals vorzubeugen, sollte in internen Regelungen festgehalten werden, dass dieser nur der Meldung von unternehmensinternen Missständen oder strafrechtlichen Verstößen genutzt werden darf; Ausschluss von Gejammer und Eifersüchteleien…;

Datenschutz und Hinweisgebersysteme

- Transparenz: Unterrichtung des Hinweisgebers

- Im Rahmen eines internen Meldesystems soll dem Hinweisgeber innerhalb von 7 Tagen nach Eingang der Meldung dieser Eingang bestätigt werden, Art. 9 Abs. 1 lit. c der RL
- Gemäß Art. 16 der RL soll die Identität des Hinweisgebers ohne dessen ausdrückliche Zustimmung keinen anderen Personen als gegenüber den befugten Mitarbeitern, die für die Entgegennahme von Meldungen oder für das Ergreifen von Folgemaßnahmen zu Meldungen zuständig sind, offengelegt werden

Datenschutz und Hinweisgebersysteme

- Eine Ausnahme gilt nur, wenn dies eine notwendige und verhältnismäßige Pflicht im Rahmen der Untersuchungen durch nationale Behörden oder von Gerichtsverfahren darstellt (also z. B. auch zur Wahrung der Verteidigungsrechte der betroffenen Person), vgl. Art. 16 II der WBRL (Katastrophe? Problem BVerfG zu Jones Day zum Beschlagnahmerecht)
- Unterrichtung über Konsequenzen bei offensichtlichem Missbrauch
- Anonymität zulässig! (entgegen Auffassung des DSK zum „Denunziantentum“), allerdings Aufklärung, dass evtl. zwingend „durchhaltbar“ (Abhängig von der Qualität der Hinweise)

Datenschutz und Hinweisgebersysteme

– Pflicht zur Benachrichtigung des Betroffenen nach 1 Monat wegen Art. 14 Abs. 3 lit. a DSGVO?

Nein, da über Art. 14 Abs. 5 b lösbar (Verarbeitung würde Ziel unmöglich machen), dann geeigneter Schutz über Benachrichtigung nach Wegfall der Ermittlungsmaßnahmen (strittig, wann Wegfall!);

andere Ansicht Art. 23 Abs. 1 lit i iVm. § 29 BDSG (Geheimhaltung bei Drittinteresse)

Datenschutz und Hinweisgebersysteme

- Information über Einwilligungsregeln des Art. 7 III DSGVO, also Widerruf

(aber nur binnen Monatsfrist wegen Art. 14 III? Zirkelschluss? Also keine Widerrufsfrist?, besser doch!)

Datenschutz und Hinweisgebersysteme

Transparenz: Auskunftsrecht des Betroffenen?

Auskunftsrecht nach Art 15 Abs. 1, Abs. 3

nein, wegen Art. 23 Abs. 1 lit. d und lit. I iVm § 29 Abs. 1 S. 2 BDSG

Dokumentation der 29er Gründe! Erinnerung an LAG BW…

Datenschutz und Hinweisgebersysteme

- Grundsatz der Datensparsamkeit
  - Spielen sensible Daten für die Meldung keine Rolle, dürfen sie nicht erwähnt werden
  - Falls diese Daten dennoch mitgeteilt werden, sind sie im weiteren Verlauf nicht in der Fallakte zu erfassen (z. B. meldet ein Hinweisgeber, dass sein Kollege Büroutensilien gestohlen hat und äußert sich über dessen Gesundheitszustand)
  - Eingrenzung relevanter Personenkreise

Datenschutz und Hinweisgebersysteme

- Mitarbeiterschulung und -sensibilisierung
  - Diejenigen Mitarbeiter („unparteiische Person“), die die Berichte oder Meldungen bearbeiten sollen (also die Folgemaßnahmen betreuen), sind hinsichtlich der datenschutzrechtlichen Vorgaben sensibilisiert und geschult
  - Die für die Bearbeitung zuständigen Mitarbeiter sollten einer zusätzlichen (vertraglichen) Geheimhaltungspflicht unterliegen

Vor allem aber vertraglicher Schutz gegenüber Herausgabeanspruch, Budget für Beauftragung Sonderprüfer

Datenschutz und Hinweisgebersysteme

Sicherheitsmaßnahmen

- Technische Maßnahmen für sicheren Datentransfer
- Werden im Zusammenhang mit der Meldung von Missständen personenbezogene Daten zu statistischen Zwecken erhoben, sollten diese anonymisiert werden
- Hinweisübermittlung sollte über einen verschlüsselten Kanal erfolgen

Datenschutz und Hinweisgebersysteme

Löschkonzept

- Unvollständige oder überholte Daten sind durch org. Maßnahmen den Löschregeln oder Berichtigungsregeln unterziehen;
- Stufenplan: falsche Daten, nicht verwendbare Daten sofort, verwendbare Daten 2 Monate nach Abschluss der Untersuchung, darüber hinaus nur wenn Einleitung Straf- oder Disziplinarverfahren

Datenschutz und Hinweisgebersysteme

Externe Dienstleister:

- Auftragsverarbeitungsvereinbarung und Kontrollen im Sinne des Art. 28 DSGVO, wenn nur it-gestütztes Verfahren
- Nach DSK bei „Funktionsübertragung“ (Anwaltskanzleien) auch DSFA

To Dos

- Aufbau vertrauliches Meldesystem
- Code of Conduct/Richtlinie Hinweisgebersystem:
  - Kontaktdaten der Meldestelle,
  - Meldeberechtigung und zulässige Meldeinhalte, Belehrung Hinweisgeber
  - Grenzen des Hinweisrechts/Konsequenzen falscher Informationen,
  - Beschreibung Meldeprozess
- Einbeziehung DSB, Compliance, Revision, Betriebsrat und …
- Compliance-Richtlinie für das Ermittlungsverfahren ab Kenntnis der gemeldeten Inhalte, auch Schutz der Ermittler

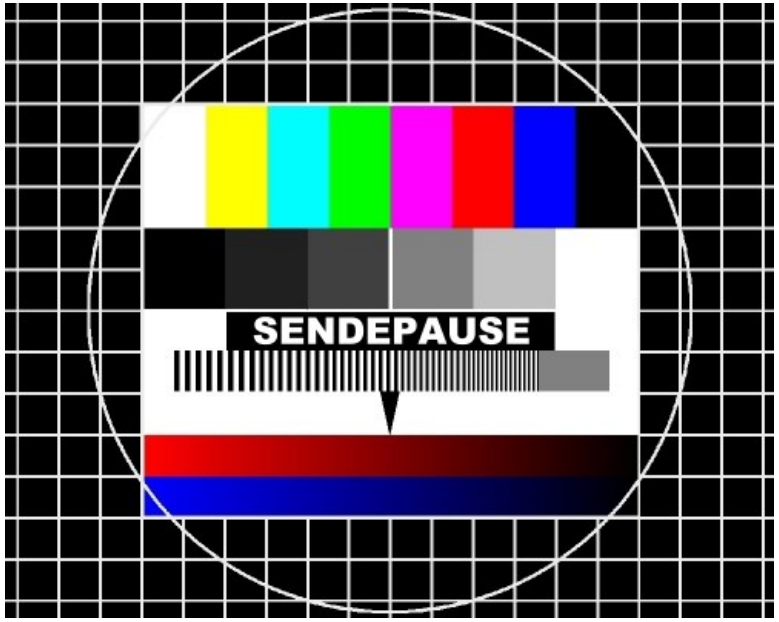
Gerne noch Fragen!

Broschüre „Prüfliste und Maßnahmen bis zum 17.12.2021“

oder

Details und Anmeldeunterlagen zum Tages-Workshop „Einrichtung und Betrieb von Hinweisgebersystemen“ ab dem 25.11.2021

sehr gerne anfordern bei kerstin.schwendrat@schmid-frank.de hier in unserer Kanzlei!



Vielen Dank!

Ihr Wolfgang Schmid

Partner der
Schmid Frank Rechtsanwälte PartG mbB
Katharinengasse 11 b
86150 Augsburg

Telefon 0821 – 4540543 (Assistentin Frau Schwendrat)
Fax 0821 - 4540680
Mobil 0172 – 8303354
wolfgang.schmid@schmid-frank.de
www.schmid-frank.de