audatis
Datenschutz und Informationssicherheit | CONSULTING

Whitepaper

Einführung eines Whistleblowing-Systems im Unternehmen unter Berücksichtigung der Anforderungen des Datenschutzes

Zusammenfassung

Mit Verabschiedung der EU-Richtlinie 2019/1937 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden („EU-Richtlinie 2019/1937“) am 23.10.2019 und der Pflicht zur Umsetzung der Richtlinie ins mitgliedsstaatliche Recht bis zum 17.12.2021 wird die Implementierung eines unternehmensseitigen Whistleblowing-Systems zur Meldung von Rechtsverletzungen des Unternehmens grundsätzlich für alle juristische Personen ab 50 Arbeitnehmern zukünftig zur Rechtspflicht.

Wie die diversen Stellungnahmen deutscher und europäischer Datenschutzbehörden und -gremien aufzeigen[1], kann die Implementierung eines Whistleblowing-Systems nicht ohne Berücksichtigung der Anforderungen des Datenschutzes erfolgen, soll das Whistleblowing-System nicht selbst zum Compliance-Risiko werden.

Problemstellung

Es sind besondere Anstrengungen zum sicheren technischen und organisatorischen Betrieb des Whistleblowing-Systems erforderlich. Auch ist die Legitimierung (Rechtmäßigkeit) der Verarbeitung personenbezogener Daten im Rahmen des Whistleblowing-Systems besonders sorgfältig zu prüfen. Der Schwerpunkt der datenschutzrechtlichen Problematik erwächst jedoch aus den widerstreitenden Interessen des Whistleblowers an der Wahrung der Vertraulichkeit seiner Identität und den Betroffenenrechten der beschuldigten Person, hier insbesondere jenen auf Information und Auskunft.

Jedes Unternehmen, das die Implementierung eines Whistleblowing-Systems anstrebt – sei es aus gesetzlicher Notwendigkeit oder als Teil eines Compliance-Management-Systems – steht damit vor der Herausforderung, das beschriebene Spannungsverhältnis aufzulösen und einen Weg zur datenschutzkonformen Erfüllung der Anforderungen der EU-Richtlinie 2019/1937 bei gleichzeitiger Sicherstellung der Wirksamkeit des Whistleblowing-Systems zu finden.

Lösungsansatz

Der richtige Weg hierzu dürfte – so auch die Auffassung der Datenschutzkonferenz[2] – über eine Datenschutz-Folgenabschätzung zur Einführung des Whistleblowing-Systems führen. Diese sollte sich insbesondere mit den folgenden Themen befassen:

1. **Der Auswahl des Meldekanals:** Gleichermaßen aus Sicht der EU-Richtlinie 2019/1937 wie auch aus Sicht der DS-GVO ist die Auswahl eines sicheren Meldekanals zentrale Anforderung des rechtmäßigen Betriebs eines Whistleblowing-Systems. Ein Briefkasten oder E-Mail-Postfach dürften dieser Anforderung kaum genügen. Sollte ein Dienstleister mit der Bereitstellung des Meldekanals beauftragt werden, sollte zudem darauf geachtet werden, dass insoweit möglichst kein Drittlandsbezug besteht, um das hieraus nach der Entscheidung des EUGH in Sachen Schrems-II erwachsende zusätzliche Risiko zu vermeiden.

[1] Artikel-29-Datenschutzgruppe, Stellungnahme 1/2006; Datenschutzkonferenz, Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines; Düsseldorfer Kreis, Arbeitsbericht der Ad-hoc Arbeitsgruppe Beschäftigtendatenschutz des Düsseldorfer Kreises; European Data Protection Supervisor, Leitlinien zur Verarbeitung personenbezogener Informationen im Rahmen eines Verfahrens zur Meldung von Missständen.

[2] Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines.

2. **Der Erfüllung der Informationspflichten:** Auch im Rahmen des Betriebs eines Whistleblowing-Systems unterliegt jedes Unternehmen den Transparenzpflichten der DS-GVO. Über die mit der Entgegennahme einer Meldung verbundene Verarbeitung personenbezogener Daten sind die betroffenen Personen daher entsprechend Art. 13, 14 DS-GVO zu informieren.

   Während sich die Erfüllung der Informationspflicht gegenüber dem Whistleblower noch vergleichsweise einfach gestaltet, entsteht hier im Verhältnis zu den beschuldigten Personen zwingend ein Spannungsverhältnis zwischen der Transparenzpflicht und dem Geheimhaltungsinteresse des Unternehmens.

   Eine vorzeitige Information, grundsätzlich sieht die DS-GVO eine Frist von einem Monat vor, kann den Erfolg der Ermittlungen gefährden – die gewarnten Beschuldigten können Beweise vernichten und Zeugen beeinflussen. Die Definition eines klaren Vorgehens, dass insbesondere eine Abwägung zwischen Information und Geheimhaltung im Einzelfall und die Erstellung einer dokumentierten Begründung vorsieht, ist damit zwingend erforderlich.

3. **Der Pflicht zur Löschung abgeschlossener Fälle:** Die Rechtspflicht des Unternehmens, einen abgeschlossenen Fall binnen zwei Monaten nach dessen Beendigung zu löschen, sofern keine rechtlichen Schritte eine längere Aufbewahrung rechtfertigen, ist der Grundstein eines Spannungsverhältnisses zwischen Datenschutz und Compliance-Anforderungen.

   Eine Löschung abgeschlossener Fälle setzt Unternehmen dem Risiko aus, bei Anfragen der Medien keinen Nachweis über durchgeführte Untersuchungen vorlegen zu können. Im Fall arbeitsrechtlicher Auseinandersetzungen – beispielsweise im Kündigungsfall – kann nicht der Nachweis geführt werden, dass die ergriffenen Maßnahmen nicht auf eine vorherige Tätigkeit des Mitarbeiters als Whistleblower zurückzuführen sind.

   Die bewusste Definition von Löschfristen und die Prüfung der Möglichkeiten zur Anonymisierung / Pseudonymisierung sollte daher ebenso Teil einer Datenschutz-Folgenabschätzung sein, wie die Abwägung des Risikos zwischen dem Eingriff in die Grundrechte der von einer Meldung betroffenen Personen und der Verschlechterung der Beweislage sowie der Erschwerung der Compliance-Arbeit.

4. **Dem Umgang mit dem Recht auf Auskunft und Erstellung einer Kopie:** Das Recht auf Auskunftserteilung unter Bereitstellung einer Kopie der verarbeiteten personenbezogenen Daten erstreckt sich grundsätzlich auch auf diejenigen personenbezogenen Daten, die im Rahmen eines Whistleblowing-Systems verarbeitet werden.

   Dies wird insbesondere dann problematisch, wenn es die beschuldigte Person ist, die ein Auskunftsverlangen geltend macht. In diesem Fall ist dem verantwortlichen Unternehmen unter Umständen zumindest die Beschränkung der Auskunft zum Schutz des Whistleblowers sowie aus Geheimhaltungsinteressen möglich. Dies setzt jedoch voraus, dass durch das Unternehmen substantiiert begründet werden kann, warum die Auskunft hinsichtlich bestimmter Informationen verweigert wird. Eine vollständige Verweigerung der Auskunft dürfte hingegen – insbesondere bei lediglich pauschaler Behauptung bestehender Geheimhaltungsinteressen – keineswegs genügen, um die Auskunft zu verweigern.

   Mit Blick auf die umfassenden Anforderungen der EU-Richtlinie 2019/1937 und die sich hieraus ergebenden Implikationen aus Sicht des Datenschutzes, ist jedem Unternehmen

mit mehr als 50 Arbeitnehmern daher zu empfehlen, sich möglichst zeitnah mit dem entstehenden Umsetzungs- und Anpassungsbedarf zu befassen.

Autor und Ansprechpartner

Jannik Wallbaum
Senior Legal Consultant Datenschutz

Schwerpunkte: Internationaler Datenschutz, Datenschutzrecht, Compliance und Risikomanagement

Mail: j.wallbaum@audatis.de
Fon: 05221 87292-09

Haben Sie noch Fragen?

Wir haben versucht, alle wichtigen Aspekte in unserem Whitepaper möglichst verständlich aufzubereiten.

Sollten Sie dennoch Fragen oder Beratungsbedarf haben, nehmen Sie gerne mit uns Kontakt auf.

Wir unterstützen Sie gerne bei der Umsetzung von internationalen Datenschutzvereinbarungen, der Betreuung von internationalen Unternehmensgruppen und der Beantwortung aller Fragen in Bezug auf die pragmatische Umsetzung der Anforderungen des EU-Datenschutzes und der Informationssicherheit.

Die audatis Consulting GmbH ist als Beratungsunternehmen auf die Bereiche Datenschutz und Informationssicherheit spezialisiert und betreut Kunden im In- und Ausland bereits seit 2011.

Neben der Stellung des externen Datenschutzbeauftragten begleiten und beraten wir Unternehmen, öffentliche Stellen und kirchliche Einrichtungen bei der Umsetzung des Datenschutzes, der Informationssicherheit und der Digitalisierung.

Als Teil der audatis Group hat die audatis Consulting GmbH Ihren Sitz im ostwestfälischen Herford und betreibt eine Niederlassung in Potsdam.

audatis Datenschutz und Informationssicherheit CONSULTING

audatis Consulting GmbH
Luisenstr. 1
32052 Herford
Deutschland

Fon: 05221 872 92-0
Fax: 05221 872 92-49

Mail: info@audatis.de
Web: www.audatis.de