Bundesamt
für Justiz

POSTANSCHRIFT Bundesamt für Justiz, 53094 Bonn

ULD – Unabhängiges Landeszentrum
für Datenschutz Schleswig-Holstein
Postfach 71 16
24171 Kiel

Externe Meldestelle des Bundes

HAUSANSCHRIFT Adenauerallee 99-103, 53113 Bonn
POSTANSCHRIFT 53094 Bonn
BEARBEITET VON [redacted]

TEL +49 228 99 410-6644
E-MAIL hinweisgeberstelle@bfj.bund.de
AKTENZEICHEN **2023 0000 1993**
(bitte immer angeben)

DATUM Bonn, 14. August 2024

BETREFF **Meldung nach dem Hinweisgeberschutzgesetz (HinSchG)**

HIER Abgabe zwecks weiterer Untersuchungen gemäß § 29 Absatz 2 Nummer 4 Hinweisgeberschutzgesetz (HinSchG)

ANLAGEN Formblatt für Eingangsbestätigung

Sehr geehrte Damen und Herren,

bei der externen Meldestelle des Bundes ist eine Meldung nach dem Gesetz für einen besseren Schutz hinweisgebender Personen (Hinweisgeberschutzgesetz – HinSchG) eingegangen. Zwecks weiterer Untersuchungen in eigener Zuständigkeit gebe ich das betreffende Verfahren gemäß § 29 Absatz 2 Nummer 4 HinSchG an Sie ab.

Das Hinweisgeberschutzgesetz soll es hinweisgebenden Personen ermöglichen, ohne Angst vor Repressalien auf Rechts- und Regelverstöße in Unternehmen und Behörden aufmerksam zu machen. Hinweisgebende Personen werden im beruflichen Umfeld durch das Gesetz umfassender als zuvor geschützt, indem gegen sie gerichtete berufliche Repressalien verboten wurden (§ 36 HinSchG).

Der Bund hat beim Bundesamt für Justiz eine Stelle für externe Meldungen (externe Meldestelle des Bundes, § 19 HinSchG) errichtet. Erhält die externe Meldestelle des Bundes eine Meldung, prüft sie, ob der persönliche und sachliche Anwendungsbereich des HinSchG eröffnet ist und ob die Meldung stichhaltig ist (§ 28 Absatz 2 HinSchG). Ist dies der Fall, kann

sie als eine mögliche Folgemaßnahme das Verfahren an eine zuständige Behörde zwecks weiterer Untersuchungen abgeben (§ 29 Absatz 2 Nummer 4 HinSchG).

Hervorzuheben ist, dass die externe Meldestelle des Bundes nach dem HinSchG einem besonderen Vertraulichkeitsgebot unterliegt. Sie darf die Identität der hinweisgebenden Person, der Personen, die Gegenstand der Meldung sind, und der sonstigen in der Meldung genannten Personen grundsätzlich nicht mitteilen, wenn sie ein Verfahren zwecks weiterer Untersuchungen abgibt (§ 8 HinSchG). Diese Informationen sowie auch solche, aus denen Rückschlüsse hierauf möglich sind, teilt die externe Meldestelle des Bundes bei Abgabe eines Verfahrens daher in der Regel zunächst nicht mit. Vielmehr werden in einem ersten Schritt grundsätzlich die um diese Informationen gekürzte Sachverhaltsdarstellungen und gegebenenfalls geschwärzte Dokumente übermittelt.

Um den zuständigen Behörden eine Untersuchung des Sachverhalts zu ermöglichen, sieht das HinSchG in § 9 verschiedene Ausnahmen von dem besonderen Vertraulichkeitsgebot vor. Informationen über die Identität der hinweisgebenden Person oder über sonstige Umstände, die Rückschlüsse auf die Identität dieser Person ermöglichen, können aufgrund einer Anordnung in einem einer Meldung nachfolgenden Verwaltungsverfahren, einschließlich verwaltungsbehördlicher Bußgeldverfahren, mitgeteilt werden (§ 9 Absatz 2 Nummer 2 HinSchG). Gleiches gilt für Personen, die Gegenstand einer Meldung sind und für sonstige in der Meldung genannte Personen (§ 9 Absatz 4 Nummer 5 HinSchG). Hier ist eine Weitergabe auch möglich, sofern dies für das Ergreifen von Folgemaßnahmen erforderlich ist (§ 9 Absatz 4 Nummer 3 HinSchG).

Die Entscheidung, ob und in welchem Umfang es für Ihr Verfahren erforderlich ist, weitere Informationen anzufordern, obliegt Ihnen als zuständiger Behörde.

<u>Dies vorangestellt, schildere ich im Folgenden das gemäß § 29 Absatz 2 Nummer 4 HinSchG abgegebene Verfahren:</u>

Eine hinweisgebende Person hat sich mit einer Meldung an die externe Meldestelle des Bundes gewandt. Gegenstand der Meldung ist der Betreiber eines Rechenzentrums in Ihrem Zuständigkeitsbereich (im Folgenden: Betreiber). Die Meldung betrifft mögliche Verstöße gegen die Datenschutz-Grundverordnung (DSGVO).

Die externe Meldestelle des Bundes hat bereits gemäß § 29 Absatz 1 Satz 1, Absatz 2 Nummer 1 HinSchG Kontakt zu dem Betreiber aufgenommen und ihn um Auskunft zu

den in der Meldung angesprochenen Punkten gebeten. Der Betreiber hat zu diesen Punkten Stellung genommen. Die hinweisgebende Person hatte Gelegenheit, auf die Stellungnahme des Betreibers zu erwidern. Demnach stellt sich der Sachverhalt folgendermaßen dar:

1. Die hinweisgebende Person nimmt in der Meldung unter anderem Bezug auf zwei Prüfberichte zu einem Projekt (Projekt 1), in denen – zum Teil schwerwiegende – Mängel festgestellt wurden (Berichte a und b). Der Betreiber wurde um Auskunft gebeten, ob diese Mängel inzwischen behoben wurden und, wenn ja, wie die Behebung der Mängel erfolgte.

   Der Betreiber teilt zu Bericht a mit, dass der Bericht zum Teil auf vom Auditor unvollständig erhobenen Sachverhalten basiere und dass folglich die daraus abgeleiteten Ergebnisse fehlerbehaftet gewesen seien. Ursächlich hierfür sei gewesen, dass – entgegen allen Gepflogenheiten im Rahmen eines Audit – der Auditor vor der Finalisierung des Berichts keinerlei Abstimmung zur sachlichen Richtigkeit der von ihm zugrunde gelegten Faktenbasis auf Basis eines Berichtsentwurfes mit dem Betreiber durchgeführt habe. Der Betreiber habe nach Kenntniserlangung des finalen Berichts gegenüber dem Auftraggeber des Projekts wie auch gegenüber einer weiteren an dem Projekt beteiligten Stelle entsprechende Stellungnahmen erstellt, um den Sachverhalt richtig zu stellen. Zudem beträfen nicht alle Prüfpunkte dieses Audit die Verantwortungssphäre des Betreibers. Die den Betreiber auf Basis des korrekten Sachverhaltes betreffenden Feststellungen seien bis Mitte 2022 vollständig und abschließend bearbeitet worden, und die Umsetzung sei dem Auftraggeber sowie der weiteren an dem Projekt beteiligten Stelle berichtet worden.

   Zu Bericht b teilt der Betreiber mit, dieser nachfolgend durchgeführte PEN-Test enthalte Feststellungen, welche insbesondere die Auftragslage zur Modernisierung eingesetzter technischer Komponenten beträfen – insoweit sei der Betreiber als Auftragsverarbeiter an explizite Vorgaben seiner Auftraggeber gebunden – sowie Feststellungen, welche die weitere Optimierung der Konfiguration und der Abläufe beim Betrieb des in Rede stehenden Verfahrens beträfen. Insoweit beschrieben die Feststellungen das Erfordernis der Weiterentwicklung der betriebsrelevanten IT zutreffend als einen kontinuierlichen Prozess zur Anpassung an gestiegene Anforderungen, an die technische Entwicklung und an die sich verändernde Risikosituation. Dieser Anpassungs- und Weiterentwicklungsprozess sei originärer Bestandteil eines jeden Verfahrensbetriebs.

Die hinweisgebende Person erwidert, dass sich diese Angaben nicht mit dem deckten, was die weitere an dem Projekt beteiligte Stelle in einem von der hinweisgebenden Person angestrengten Beschwerdeverfahren der für diese Stelle zuständigen Datenschutzaufsichtsbehörde mitgeteilt habe. Demnach habe die weitere an dem Projekt beteiligte Stelle dem Betreiber im Mai 2022 eine Frist zur Behebung der Mängel bis zum 1. November 2022 gesetzt. Im November 2022 sei eine Rückmeldung des Betreibers zur Behebung der Mängel erfolgt. Ein Großteil der Mängel sei behoben worden. Für die verbliebenen Mängel sei ein Sachstand sowie ein Umsetzungsplan zur Behebung der Mängel angegeben und Fristverlängerung bis zum 31. Januar 2023 erbeten worden. Die weitere an dem Projekt beteiligte Stelle habe eine dringende Empfehlung zur unmittelbaren Beseitigung der Mängel ausgesprochen.

Dazu, dass der Betreiber als Auftragsverarbeiter an explizite Vorgaben seiner Auftraggeber gebunden sei, erwidert die hinweisgebende Person, dass sich dies nicht mit der Wirklichkeit decke. In aller Regel gäben in Deutschland die Auftragsverarbeiter und nicht der Verantwortliche den Vertrag vor. Dass der Betreiber Risiken ernstnehme, könne die hinweisgebende Person nicht bestätigen.

2. Die hinweisgebende Person teilt weiter mit, dass sie im Transparenzportal eines Auftraggebers des Betreibers keinen Vertrag zur Auftragsverarbeitung gemäß Artikel 28 DSGVO finden könne. Der Betreiber wurde um Auskunft gebeten, ob ein solcher Vertrag besteht.

   Der Betreiber teilt hierzu mit, dass der Auftraggeber entscheide, welche Dokumente er in das von ihm verantwortete Transparenzportal einstelle. Insofern könne der Betreiber zu diesem Aspekt nicht Stellung nehmen. Zur Klarstellung weise er aber darauf hin, dass Artikel 28 DSGVO keinen Auftragsverarbeitungsvertrag in der Form eines separaten Dokuments mit der Bezeichnung „Auftragsverarbeitungsvertrag“ fordere; Artikel 28 DSGVO fordere vielmehr, dass die für die Auftragsverarbeitung maßgeblichen datenschutzrechtlichen Regelungen vertraglich zwischen dem Verantwortlichen und dem Auftragsverarbeiter vereinbart werden. Der Standardvertrag des Betreibers inklusive seiner Anlagen, insbesondere der Vertragsbedingungen Auftragsverarbeitung als Bestandteil der Allgemeinen Vertragsbedingungen des Betreibers, sei zugleich Leistungs- bzw. Hauptvertrag und Auftragsverarbeitungsvertrag. Der Standardvertrag des Betreibers entspreche inhaltlich vollumfänglich den

Anforderungen der DSGVO, was auch von der für den Betreiber zuständigen Datenschutzaufsicht anerkannt werde. Ein gesondertes Vertragsdokument „Auftragsverarbeitungsvertrag“ erübrige sich daher.

Die hinweisgebende Person erwidert, die Vertragsbedingungen Auftragsverarbeitung des Betreibers erfüllten die Mindestanforderungen aus Artikel 28 Absatz 3 Buchstabe c DSGVO nicht. Nach Kenntnis der hinweisgebenden Person existierten daneben sogenannte Security Service Level Agreements. Diese enthielten ebenfalls lediglich Absichtserklärungen und keine konkreten technischen und organisatorischen Maßnahmen.

3. Die hinweisgebende Person äußert die Vermutung, dass kein Verzeichnis von Verarbeitungstätigkeiten (Artikel 30 DSGVO) bestehe. Der Betreiber wurde um Auskunft gebeten, ob ein solches Verzeichnis besteht.

   Der Betreiber weist hierzu zunächst darauf hin, dass es ein Verzeichnis von Verarbeitungstätigkeiten (VVT) sowohl gemäß Artikel 30 Absatz 1 DSGVO als auch gemäß Artikel 30 Absatz 2 DSGVO gebe. Ersteres habe der Verantwortliche (der Auftraggeber bzw. Kunde des Betreibers) zu erstellen, und insoweit sei dem Betreiber eine Auskunft nicht möglich. Das vom Betreiber als Auftragsverarbeiter gemäß Artikel 30 Absatz 2 DSGVO zu erstellende VVT liege vor.

   Die hinweisgebende Person weist in ihrer Erwiderung darauf hin, dass der Betreiber das VVT nicht vorgelegt hat.

4. Schließlich macht die hinweisgebende Person allgemein Bedenken hinsichtlich der Sicherheit eines weiteren Projekts (Projekt 2) geltend. Hierzu wurde dem Betreiber Gelegenheit zur Stellungnahme gegeben.

   Der Betreiber hat hierzu mitgeteilt, dass es ihm nicht möglich sei, zu einer derart pauschalen und unsubstantiierten Geltendmachung von „Bedenken hinsichtlich der Sicherheit“ Stellung zu nehmen. Dessen ungeachtet weise er darauf hin, dass er IT-Verfahren grundsätzlich auf Basis eines BSI-Grundschutz-konformen Sicherheitskonzepts betreibe. Ergänzend verweise er auf die ihm durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) erteilten ISO 27001-Zertifikate auf der Basis von IT-Grundschutz.

Die hinweisgebende Person erwidert, die Antwort des Betreibers sei irreführend. Die Rechenzentren des Betreibers seien zertifiziert, und das auf niedrigstem Niveau. Dass ein dort betriebenes Verfahren im Sinne von Anwendungssoftware zertifiziert sei, sie ihr nicht bekannt.

Ich rege an, die Angaben des Betreibers zu den oben angesprochenen Punkten zu überprüfen, um sie gegebenenfalls zu bestätigen.

Die hinweisgebende Person hat in die Weitergabe von Informationen über ihre Identität eingewilligt. Gemäß § 9 Absatz 3 HinSchG teile ich Ihnen daher mit, dass es sich bei der hinweisgebenden Person handelt um:

Herrn Joachim Lindenberg
Heubergstraße 1a, 76228 Karlsruhe

Eine E-Mail-Adresse der hinweisgebenden Person kann ich Ihnen – wegen der Bestimmung des § 8 Absatz 1 Satz 1 Nummer 2 HinSchG – erst auf Anforderung übermitteln.

Nach § 31 Absatz 6 HinSchG muss die externe Meldestelle des Bundes der hinweisgebenden Person das Ergebnis der durch die Meldung ausgelösten Untersuchungen nach deren Abschluss mitteilen, soweit dies mit gesetzlichen Verschwiegenheitsverpflichtungen vereinbar ist. Ich bitte daher darum, mir bei Abschluss Ihres Verfahrens einen aussagekräftigen Antwortbeitrag zu übersenden, den ich an die hinweisgebende Person weiterleiten darf. Dies vermeidet, dass Verschwiegenheitsverpflichtungen verletzt werden. Des Weiteren komme ich damit meiner Auskunftspflicht gegenüber der hinweisgebenden Person nach.

Da ich nach § 26 HinSchG verpflichtet bin, den weiteren Gang des Verfahrens zu verfolgen, bitte ich Sie, mich über den Fortgang Ihres Verfahrens zu informieren.

Damit Ihre Zuschriften direkt und ohne Einbindung einer anderen Stelle im Bundesamt für Justiz der externen Meldestelle des Bundes zugeleitet werden können, adressieren Sie Ihre Schreiben bitte stets ausdrücklich an folgende Adresse:

Bundesamt für Justiz
- Externe Meldestelle des Bundes –
53094 Bonn

oder nutzen Sie unsere EGVP-Adresse:

egvp_Hinweisgeberstelle@bfj.intern

Abschließend bitte ich Sie, auf dem beiliegenden Formblatt den Eingang meines Schreibens zu bestätigen und mir Ihr Aktenzeichen mitzuteilen.

Für Rückfragen stehe ich Ihnen gerne zur Verfügung.

Mit freundlichen Grüßen
Im Auftrag

[redacted]