Bundesamt
für Justiz

POSTANSCHRIFT Bundesamt für Justiz, 53094 Bonn

Herrn
Joachim Lindenberg

Externe Meldestelle des Bundes

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

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

Per E-Mail:
[redacted]**@lindenberg.one**

DATUM Bonn, 29. April 2024

BETREFF **Meldung nach dem Hinweisgeberschutzgesetz**

HIER Weiteres Vorgehen – Abgabe des Verfahrens an die Landesbeauftragte für Datenschutz Schleswig-Holstein (Unabhängige Landeszentrum für Datenschutz)

Sehr geehrter Herr Lindenberg,

haben Sie vielen Dank für Ihre Nachricht vom 23. Februar 2024. Wie angekündigt, beabsichtige ich, das Verfahren gemäß § 29 Absatz 2 Nummer 4 HinSchG zwecks weiterer Untersuchungen an die Landesbeauftragte für Datenschutz Schleswig-Holstein (Unabhängige Landeszentrum für Datenschutz) abzugeben.

Bitte beachten Sie dazu folgende Hinweise:

Die externe Meldestelle des Bundes wahrt die Vertraulichkeit der Identität der hinweisgebenden Person (§ 8 Absatz 1 Nummer 1 HinSchG), also die Vertraulichkeit Ihrer Identität. Dies betrifft auch sonstige Umstände, die Rückschlüsse auf die Identität der hinweisgebenden Person erlauben. Anderen Behörden, an die wir ein Verfahren zwecks weiterer Untersuchungen gemäß § 29 Absatz 2 Nummer 4 HinSchG abgeben (z.B. eine Aufsichtsbehörde), bringen wir deshalb in einem ersten Schritt nur eine anonymisierte und umformulierte Textfassung der Meldung zur Kenntnis. Beachten Sie aber bitte, dass die Möglichkeit besteht, dass wir Informationen über die Identität einer hinweisgebenden Person oder über

sonstige Umstände, die Rückschlüsse auf die Identität dieser Person erlauben, an die anderen Behörden weitergeben müssen, wenn diese das anordnen (§ 9 Absatz 2 Nummer 2 HinSchG). Die Akten der anderen Behörden können der Akteneinsicht unterliegen, so dass mit dem Sachverhalt vertrauten Personen auf diesem Weg Rückschlüsse auf die Identität der hinweisgebenden Person möglich sein können. Bei entsprechender Gestaltung des Sachverhalts ist es auch nicht ausgeschlossen, dass bei dem betroffenen Beschäftigungsgeber schon dann Rückschlüsse auf die Identität der hinweisgebenden Person möglich sind, wenn dort bekannt wird, dass Aufsichtsmaßnahmen eingeleitet worden sind.

Die externe Meldestelle des Bundes ist zudem zum Schutz der Personen verpflichtet, die Gegenstand einer Meldung sind. Daher könnte die Landesbeauftragte für Datenschutz Schleswig-Holstein durch uns zum Sachverhalt zunächst folgendermaßen informiert werden:

> „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 Audi-

tor 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 Angaben zur Identität des betroffenen Betreibers und zu den betroffenen Projekten wird die externe Meldestelle des Bundes der Landesbeauftragten für Datenschutz Schleswig-Holstein auf Anforderung übermitteln (§ 9 Absatz 4 Nummer 3 und 5 HinSchG).

Sie können Vorschläge für alternative Formulierungen machen, falls Ihnen die obige Sachverhaltsschilderung hinsichtlich Ihrer Äußerungen nicht zutreffend erscheint oder Sie der Ansicht sind, dass andere Formulierungen besser geeignet sind, um Ihre Identität zu schützen.

Sie erhalten Gelegenheit, sich zu den genannten Gesichtspunkten bis zum

27. Mai 2024

zu äußern.

Mit freundlichen Grüßen
Im Auftrag
[redacted]