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, 8. Dezember 2023

BETREFF **Meldung nach dem Hinweisgeberschutzgesetz**

HIER Weitere Rückmeldung gemäß § 28 Absatz 4 Hinweisgeberschutzgesetz und Anhörung gemäß § 28 Absatz 1 Verwaltungsverfahrensgesetz

BEZUG Ihr Schreiben vom 28. September 2023

Sehr geehrter Herr Lindenberg,

für Ihr Schreiben vom 28. September 2023 danke ich Ihnen. Einige Punkte sind leider immer noch klärungsbedürftig:

1. Ob es sich bei der Dataport AöR bzw. den von ihr betriebenen Anlagen, auf die sich Ihre Meldung bezieht, um Kritische Infrastruktur im Sinne der BSI-Kritisverordnung handelt, muss aufgeklärt werden.

   Es ist richtig, dass § 5 Absatz 1 Nummer 1 Hinweisgeberschutzgesetz (HinSchG) die Bestimmung des Artikel 3 Absatz 2 der Richtlinie (EU) 2019/1937 (Hinweisgeberschutz-Richtlinie, HinSch-RL) aufgreift. Nach Artikel 3 Absatz 2 Satz 1 HinSch-RL berührt die Richtlinie nicht die Verantwortung der Mitgliedstaaten, die nationale Sicherheit zu gewährleisten, oder ihre Befugnis zum Schutz ihrer wesentlichen Sicherheitsinteressen. Dementsprechend bestimmt § 5 Absatz 1 Nummer 1 HinSchG, dass eine Meldung nicht in den Anwendungsbereich des HinSchG fällt, wenn sie Informationen beinhaltet, die die nationale Sicherheit oder wesentliche Sicherheitsinteressen des Staates, insbesondere

militärische oder sonstige sicherheitsempfindliche Belange des Geschäftsbereiches des Bundesministeriums der Verteidigung oder Kritische Infrastrukturen im Sinne der BSI-Kritisverordnung betreffen. Der Gesetzgeber geht also davon aus, dass dann, wenn Informationen Kritische Infrastrukturen im Sinne der BSI-Kritisverordnung betreffen, stets die nationale Sicherheit oder wesentliche Sicherheitsinteressen des Staates betroffen sind. Diese Wertung des Gesetzgebers ist angesichts der Definition der Kritischen Infrastrukturen in § 2 Absatz 10 Satz 1 BSI-Gesetz auch nachvollziehbar. Demnach sind Kritische Infrastrukturen Einrichtungen, Anlagen oder Teile davon, die bestimmten Sektoren, unter anderem dem Sektor Informationstechnik und Telekommunikation, angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Die nähere Bestimmung erfolgt durch die BSI-Kritisverordnung (§ 2 Absatz 10 Satz 2 BSI-Gesetz). Damit schließt § 5 Absatz 1 Nummer 1 HinSchG nicht jede Datenverarbeitung in einem Rechenzentrum vom Anwendungsbereich des HinSchG aus, sondern nur die Datenverarbeitung in Rechenzentren, die die in meinem Schreiben vom 20. September 2023 genannten Schwellenwerte nach der BSI-Kritisverordnung erreichen oder überschreiten und daher von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Der Wille des Gesetzgebers zu einer solchen Regelung kommt in § 5 Absatz 1 Nummer 1 HinSchG eindeutig zum Ausdruck. Einen Verstoß gegen Unionsrecht kann ich darin nicht erkennen. Sollte die Regelung doch über das nach Artikel 3 Absatz 2 HinSch-RL Zulässige hinausgehen, wäre das vom Europäischen Gerichtshof festzustellen. Ein Verstoß gegen die Datenschutz-Grundverordnung (DSGVO) liegt schon deshalb nicht vor, weil § 5 Absatz 1 Nummer 1 HinSchG das Regelungs- und Aufsichtssystem der DSGVO nicht berührt.

Wären Sie zur Klärung dieses Punkts damit einverstanden, dass die externe Meldestelle des Bundes bei der Dataport AöR nachfragt, ob es sich bei den von ihr betriebenen Anlagen um Kritische Infrastrukturen im Sinne der BSI-Kritisverordnung handelt? Ihr Name und der Inhalt Ihrer Meldung würden dabei nicht genannt. Zur Erläuterung müsste der Dataport AöR aber mitgeteilt werden, dass Hintergrund der Nachfrage eine hier eingegangene Meldung nach dem HinSchG ist. Dass der Dataport AöR dann unter Umständen Rückschlüsse auf Ihre Identität möglich sind, vermag ich nicht auszuschließen.

2. Eine solche Nachfrage kommt allerdings erst dann in Betracht, wenn die in meinem Schreiben vom 20. September 2023 angesprochenen Bedenken hinsichtlich der Stichhaltigkeit der Meldung ausgeräumt sind. Ich habe darauf hingewiesen, dass unklar bleibt, worin konkret nach Ihrer Auffassung die mangelhafte Umsetzung von Artikel 32 DSGVO besteht. Weitere inhaltliche Angaben dazu haben Sie nicht gemacht. Das Schreiben des BfDI, das Sie erwähnen, lag Ihrer Nachricht nicht bei. Es trifft zu, dass nach Artikel 5 Absatz 2 DSGVO der Verantwortliche die Einhaltung der Datenschutzgrundsätze nachweisen können muss. Die externe Meldestelle des Bundes ist aber keine Aufsichtsbehörde im Sinne der DSGVO. Ihre Aufgabe ist es, wenn der Anwendungsbereich des HinSchG eröffnet ist, die Stichhaltigkeit der Meldung zu prüfen (§ 28 Absatz 2 Satz 2 HinSchG). Hierzu sind hinreichend konkrete Angaben zum mit der Meldung geltend gemachten Verstoß erforderlich, ansonsten kann die externe Meldestelle des Bundes diese gesetzliche Aufgabe nicht erfüllen.

   Sie haben Gelegenheit, innerhalb der unten genannten Frist, Angaben dazu zu machen, worin konkret bei welchem konkreten Projekt der Dataport AöR nach Ihrer Auffassung die mangelhafte Umsetzung von Artikel 32 DSGVO besteht. Werden solche Angaben innerhalb der unten genannten Frist nicht gemacht, beabsichtige ich das Verfahren durch Veraltungsakt abzuschließen, ohne weitere Folgemaßnahmen zu ergreifen.

3. Wie schon in meinem Schreiben vom 20. September 2023 ausgeführt, ist die externe Meldestelle des Bundes zu eigenen Untersuchungen mutmaßlicher Verstöße nicht befugt. Das HinSchG räumt der externen Meldestelle des Bundes keine solche Befugnis ein. Selbst wenn dies einen Verstoß gegen die HinSch-RL darstellen würde, würde sich daraus keine Befugnis der externen Meldestelle des Bundes zu solchen Untersuchungen ergeben. Hierzu bedürfte es einer vom deutschen Gesetzgeber geschaffenen Rechtsgrundlage. Eine solche existiert nicht. Würde sich die externe Meldestelle des Bundes Befugnisse anmaßen, über die sie nicht verfügt, wären rechtsstaatliche Grundsätze und im konkreten Fall auch solche der Zuständigkeitsordnung im föderalen Staat verletzt. Es bleibt dabei, dass – bei Vorliegen der Voraussetzungen – hier als weitere Folgemaßnahme die Abgabe des Verfahrens an die zuständige Behörde zwecks weiterer Untersuchungen gemäß § 29 Absatz 2 Nummer 4 HinSchG in Betracht kommt, nämlich an die Landesbeauftragte für Datenschutz Schleswig-Holstein – Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (vgl. §§ 3, 39 Landesdatenschutzgesetz Schleswig-Holstein).

Sie haben Gelegenheit zur Äußerung zu den genannten Gesichtspunkten bis zum

8. Januar 2024.

Sie können für Ihre Antwort gerne auch unser Online -Formular nutzen. Geben Sie dabei bitte im ersten Freitextfeld das oben genannte Aktenzeichen an.

Hinweis: Die Äußerung ist freiwillig. Eine Auskunftspflicht besteht nicht. Das gilt insbesondere für Auskünfte, durch die Sie sich die Gefahr zuziehen würden, wegen einer Straftat oder einer Ordnungswidrigkeit verfolgt zu werden.

Mit freundlichen Grüßen
Im Auftrag
[redacted]