Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

[redacted]

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Postfach 1468, 53004 Bonn

Physikalisch-Technische Bundesanstalt
Präsident
[redacted]
Bundesallee 100
38116 Braunschweig

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
FON (0228) 997799-[redacted]
E-MAIL Referat22@bfdi.bund.de
BEARBEITET VON [redacted]
INTERNET www.bfdi.bund.de
DATUM Bonn, 01.04.2022
GESCHÄFTSZ. 22-509/034#0316

Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

nachrichtlich:
Physikalisch-Technische Bundesanstalt
Behördlicher Datenschutzbeauftragter
[redacted]
Bundesallee 100
38116 Braunschweig

BETREFF **Beratungs- und Kontrollbesuch gemäß Artikel 57 Abs. 1 lit. a), Artikel 58 Abs. 1 lit. b) Datenschutz-Grundverordnung i.V.m. § 9 Abs. 1, § 14 Abs. 1 Nr. 1 und Nr. 4 Bundesdatenschutzgesetz**
HIER Kontrollbericht
BEZUG Kontrollankündigung vom 11. Oktober 2021

Sehr geehrter [redacted],

am 10. und 11. November 2021 habe ich eine Vor-Ort-Kontrolle bei der Physikalisch-Technischen Bundesanstalt (PTB) in Braunschweig durchgeführt.

Gegenstand meiner Kontrolle nach Art. 57 Abs. 1 lit. a), Art. 58 Abs. 1 lit. b) Datenschutz-Grundverordnung (DSGVO) i.V.m. § 9 Abs. 1, § 14 Abs. 1 Nr. 1 und Nr. 4 Bundesdatenschutzgesetz (BDSG) waren:

- Stellung und Ausstattung des behördlichen Datenschutzbeauftragten inklusive der Datenschutzorganisation
- Verpflichtung und Schulung der Mitarbeitenden
- Datenverarbeitungen bei Forschungsvorhaben

ZUSTELL- UND LIEFERANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

- Datenverarbeitungen im Zusammenhang mit der Webseite und anderer Telemedienangebote
- Erfüllung von Informationspflichten nach Art. 13 und 14 DSGVO
- Bearbeitung von Betroffenenrechten nach Kapitel III der DSGVO
- Meldung und Dokumentation von Datenschutzverletzungen nach Art. 33 und 34 DSGVO
- Einbindung von Dienstleistern und Auftragsverarbeitern, insbesondere zur Durchführung von Video-/Webkonferenzen
- Datentransfer in Drittstaaten, inkl. evtl. vorgenommener Anpassungen nach der Entscheidung des Europäischen Gerichtshofes (EuGH) in der Rechtssache C-311/18 „Schrems II“ auf der Grundlage des Informationsschreibens des BfDI vom 8. Oktober 2020

Die Kontrolle führte zu folgendem Ergebnis:

Die Kontrolle hat keine datenschutzrechtlichen Defizite ergeben.

Jedoch möchte ich vier Praxisempfehlungen aussprechen. Im Einzelnen:

1. **Schulung neuer Mitarbeitender**

Im Rahmen der Vor-Ort-Kontrolle konnten Sie auf vielfache Informationsangebote hinweisen, die den Beschäftigten der PTB zur Verfügung stehen. Eine proaktive Schulung oder Einweisung neuer Mitarbeitender in der Form einer Grundsensibilisierung für die Belange des Datenschutzes erfolgt jedoch derzeit nicht. Ich rate Ihnen daher, das vorhandene Fachwissen des behördlichen Datenschutzbeauftragten und seiner Stellvertreterin auch dafür zu nutzen, neue Mitarbeitende – ggf. gemeinsam in Sammelterminen – in kompakter und eingängiger Form zu schulen. Eine entsprechende Aufgabe des Datenschutzbeauftragten lässt sich Art. 39 Abs. 1 lit. a) DSGVO entnehmen.

2. Implementierung von Prozessen zu Betroffenenrechten

Nach Ihrer Aussage erfolgt die Bearbeitung von Betroffenenrechten nach Kapitel III der DSGVO bei Ihnen an zentraler Stelle durch das Referat Z.13 – Justiziariat. Auf Nachfrage konnten allerdings keine detaillierten Angaben zu den Prozessen gemacht werden, die bspw. bei einem Auskunftsersuchen (Art. 15 DSGVO), einer Bitte um Löschung (Art. 17 DSGVO) oder einem Widerspruch gegen die Verarbeitung (Art. 21 DSGVO) zu deren Beantwortung bei Ihnen erfolgen. Von den zuständigen Mitarbeitenden wurde daraufhin erläutert, dass die Prozesse zwar noch nicht definiert seien, im Einzelfall aber alles Notwendige veranlasst werde, um Betroffenenrechten alsbald zu entsprechen. Zum Hintergrund wurde ausgeführt, dass die Prozessdefinition in Ermangelung entsprechender Anträge noch nicht erfolgt ist.

Ich empfehle Ihnen, entsprechende Prozesse zumindest in Grundform zu implementieren. Betroffenenrechten ist nach Art. 12 Abs. 3 Satz 1 DSGVO unverzüglich, spätestens aber innerhalb eines Monats zu entsprechen. Eine Verlängerung der Bearbeitungsfrist nach Satz 2 der vorgenannten Vorschrift stellt dabei eine Ausnahme von der Regel dar, von der auch nur Gebrauch gemacht werden kann, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Die Ausnahme scheidet folglich bereits dem Wortlaut nach aus, wenn die Verzögerung auf nicht definierten Prozessen beruht.

3. Speicherdauer von Dokumentationen nach Art. 33 Abs. 5 DSGVO

Im Rahmen der Kontrolle haben Sie angegeben, dass Sie die Dokumentationen nach Art. 33 Abs. 5 DSGVO in der Regel für fünf Jahre speichern, um sich gegen etwaige Ansprüche betroffener Personen verteidigen zu können. Bei der Speicherdauer orientieren Sie sich an den Verjährungsfristen des Zivilrechts (§§ 186 ff. BGB).

Ich bitte Sie, diese Speicherdauer vor dem Hintergrund des Grundsatzes der Speicherbegrenzung nach Art. 5 Abs. 1 lit. e) DSGVO auf eine Höchstspeicherdauer von drei Jahren zu reduzieren und mir diese Anpassung zu bestätigen.

Die Frist beginnt ausweislich des Wortlauts des Art. 33 Abs. 5 DSGVO mit der Verletzung des Schutzes personenbezogener Daten und dürfte zumindest so lange andauern, wie mit einer Überprüfung der Einhaltung des Art. 33 DSGVO bzw. der Grundsätze des Art. 5 Abs. 1 lit. f) DSGVO durch die Aufsichtsbehörde (in Ihrem Fall erfolgt die Aufsicht ausschließlich durch den BfDI) zu rechnen ist. Bezüglich der Dauer kann beispielsweise eine hohe Anzahl an Meldungen nach Art. 33 Abs. 1 DSGVO ein Indiz dafür sein, dass diese zum Anlass für eine Kontrolle genommen werden, bei der dann u.a. auch die Dokumentation der Daten-

schutzverletzungen nach Art. 33 Abs. 5 DSGVO eingesehen werden soll. Dies ist bei Ihnen zumindest aktuell nicht der Fall. Diese Dauer kann sich je nach den Umständen des Einzelfalles verlängern. Verlängerungen wären beispielsweise denkbar bei laufenden Kontrollen durch die Aufsichtsbehörde oder wenn die Meldung bzw. die mit der Meldung dokumentierte Verletzung Gegenstand eines gerichtlichen Verfahrens ist oder sich ein solches unmittelbar abzeichnet, weil Ihnen gegenüber Ansprüche geltend gemacht werden.

Nach einer Aufbewahrungszeit von drei Jahren ist nach meiner Einschätzung nicht mehr damit zu rechnen, dass erstmalig Ansprüche Ihnen gegenüber geltend gemacht werden. Im Übrigen ist der primäre Zweck der Dokumentation und mithin der Speicherung derselben unmittelbar dem Gesetzeswortlaut des Art. 33 Abs. 5 Satz 2 DSGVO zu entnehmen. So dient die Dokumentation der Ermöglichung der Kontrolle der Vorgaben des Art. 33 DSGVO durch die Aufsichtsbehörde, hingegen nicht primär der Verteidigung von Rechtsansprüchen.

4. Datentransfer in Drittstaaten, unter Berücksichtigung der Entscheidung des Europäischen Gerichtshofes (EuGH) in der Rechtssache C-311/18 „Schrems II“

Sie setzen als verantwortliche Stelle unter anderem das Cisco-Webex-Videokonferenzsystem und Microsoft Teams als Online-Dienst (Software as a Service) ein, bei dem die beiden Anbieter als Auftragsverarbeiter für die PTB tätig werden. Hinsichtlich möglicher Rechtsgrundlagen für die Datenverarbeitungen auf der ersten Stufe (Kapitel II der DSGVO) stellen Sie in Ihren Datenschutzinformationen auf Art.6 Abs.1 lit. a), b), c), e) (hier in Zusammenhang mit Abs. 3 DSGVO i.V.m. § 3 BDSG und den jeweils einschlägigen Fachvorschriften) sowie Art. 88 Abs. 1 DSGVO i.V.m. § 26 Abs. 1 S. 1 BDSG im Hinblick auf die Daten Ihrer Mitarbeitenden ab. Da es auf die jeweiligen Umstände des Einzelfalls bei der Nutzung der Videokonferenzsysteme ankommt, ist das Berufen auf mehrere Rechtsgrundlagen grundsätzlich möglich.

Soweit Sie sich im Rahmen Ihrer Aufgabenerfüllung zur Erhaltung und Sicherstellung der Kommunikationsstrukturen, wie in Ihren Datenschutzinformationen angegeben, auf Art.6 Abs.1 lit. f) DSGVO berufen, ist jedoch zu berücksichtigen, dass Behörden sich bei der Erfüllung ihrer Aufgaben nicht auf Art.6 Abs.1 lit. f) DSGVO berufen können (vgl. Art.6 Abs.1 Satz 2 DSGVO) Dies möchte ich Ihnen mit auf den Weg geben und um Überarbeitung der entsprechenden Passagen in Ihren Datenschutzinformationen bitten.

Ihre Berufung auf Art. 49 Abs. 1 lit. a) DSGVO auf der zweiten Stufe (Kapitel V der DSGVO) erscheint möglich. Zwar sind die Ausnahmevorschriften eng auszulegen, dennoch werden Cisco-Webex und Microsoft Teams nach Ihrer glaubhaften Darstellung nur in Ausnahmesi-

tuationen genutzt. Für diese Einzelfälle haben Sie entsprechende Vorgaben erarbeitet und kommuniziert.

Da Sie die Übermittlung personenbezogener Daten der Teilnehmenden in die USA und auch in andere Länder außerhalb des EWR nicht ausschließen können, werden von Ihnen entsprechende Nutzungsvorgaben gemacht, die lediglich einen subsidiärer Einsatz von Cisco-Webex und Microsoft Teams vorsehen, wenn keine anderen Tools vorrangig eingesetzt werden können (absolute Notwendigkeit zur Nutzung eines bestimmten Tools).

Ich möchte Ihnen allerdings empfehlen, die entsprechenden Einwilligungserklärungen im Zusammenhang mit Art. 49 Abs. 1 lit. a) DSGVO zu überarbeiten. Neben einer ausdrücklichen Einwilligung der Betroffenen in die Weitergabe ihrer personenbezogenen Daten für den konkreten Fall sind die Betroffenen aus Nachweisgründen in der Einwilligungserklärung auch über die möglichen Risiken dieser Datenübermittlungen aufzuklären (hier: durch Hinweise auf die besonderen Risiken einer Übermittlung ihrer personenbezogenen Daten an ein Drittland wie eventuelle Zugriffe durch Sicherheitsbehörden und die eingeschränkte Möglichkeit der Ausübung von Betroffenenrechten, s. auch Leitlinien 2/2018 des Europäischen Datenschutzausschusses, S. 9). Ein weiterführender Hinweis bzgl. der Zurkenntnisnahme der Datenschutzerklärung mit entsprechender Verlinkung in der Einwilligungserklärung ist dann ein gangbarer Weg. Des Weiteren ist bitte auch noch der Hinweis mit aufzunehmen, dass die Einwilligungserklärung von der betroffenen Person jederzeit mit Wirkung für die Zukunft widerrufen werden kann (Art. 7 Abs. 3 DSGVO).

Positiv hervorheben möchte ich Ihre Datenschutzorganisation, also die Eingliederung des behördlichen Datenschutzbeauftragten und der Stabsstelle Q.01 – Sicherheit in die Gesamtorganisation. Durch die von Ihnen praktizierte Verbindung von Datenschutz und Informationssicherheit stellen Sie durch regelmäßige Schutzbedarfsfeststellungen sowie durch ein einladend gestaltetes Informationsangebot (bspw. im Intranet) eine frühzeitige Einbeziehung datenschutzrechtlicher Erwägungen sicher.

Erlauben Sie mir abschließend noch den folgenden Hinweis:

Der BfDI strebt ein modernes Informationsmanagement zwischen Bürger und Staat an, das eine Begegnung auf Augenhöhe ermöglichen soll. In Verfolgung dieses Ziels werden Kontrollberichte im rechtlich zulässigen Rahmen veröffentlicht. Sofern die kontrollierte Stelle dies wünscht, wird auch deren Stellungnahme veröffentlicht. Sofern der Kontrollbericht Namen einzelner natürlicher Personen enthält, werden diese vor Veröffentlichung ge-

schwärzt. Die Veröffentlichung erfolgt etwa einen Monat nach Übersendung des Kontrollberichts.

Sofern Sie Bedenken gegen die geplante Veröffentlichung haben, bitte ich Sie, mir diese mitzuteilen.

Über eine eventuelle Pflicht zur Herausgabe nach den Regelungen des Informationsfreiheitsgesetzes des Bundes ist im Einzelfall gesondert zu entscheiden.

Mit freundlichen Grüßen
im Auftrag
[redacted]