Bundesministerium
für Ernährung
und Landwirtschaft

**RegDir Andrea Doberstein**
Referat 111 – Verwaltungsmodernisierung,
Organisation, Bibliothek, Sprachendienst,
Digitalisierung in der Abteilung 1

Bundesministerium für Ernährung und Landwirtschaft
– Dienstsitz Berlin – 11055 Berlin

[redacted]

HAUSANSCHRIFT Rochusstraße 1, 53123 Bonn
TELEFON +49 30 18 529-0
FAX +49 30 18 529-4262
E-MAIL 111@bmel.bund.de
INTERNET www.bmel.de
GESCHÄFTSZEICHEN 111-05111/0027#001

DATUM 4. April 2022

Ausschließlich per E-Mail
[redacted]

**Antrag auf Informationszugang nach dem Informationsfreiheitsgesetz (IFG)**
Ihre E-Mail vom 31.12.2021

Sehr gee[redacted]

mit E-Mail vom 31.12.2021 beantragen Sie beim Bundesministerium für Ernährung und Landwirtschaft (BMEL) Informationen zur datenschutzrechtlichen Absicherung von Datentransfers in Drittländer.

Da Sie Informationen erbitten, die weder im Zusammenhang mit den in § 2 Absatz 1 Verbraucherinformationsgesetz (VIG) noch mit den in § 2 Absatz 3 Umweltinformationsgesetz (UIG) genannten Daten stehen, fällt Ihr Antrag nicht in den Anwendungsbereich dieser Gesetze. Ihr Antrag ist daher als Antrag auf Zugang zu Informationen nach § 1 Informationsfreiheitsgesetz (IFG) anzusehen.

Über Ihren Antrag entscheide ich nach §§ 1 Absatz 1, 10 IFG wie folgt:

I. Der Antrag wird abgelehnt.
II. Der Bescheid ergeht gebührenfrei.

Begründung:

Die nachfolgend geschilderte Gefährdungslage für die Aufrechterhaltung der vom BMEL wahrgenommenen Staats- und Regierungsfunktionen besteht bei Auskunfterteilung unabhängig davon, ob das BMEL die von Ihnen nachgefragten Aktivitäten ausgeführt hat. Aus

den Ausführungen kann daher nicht auf das Vorliegen oder Nichtvorliegen derartiger Aktivitäten geschlossen werden.

Zu I.

Es besteht kein Anspruch auf Informationszugang nach § 1 Absatz 1 Satz 1 IFG. Danach hat jeder nach Maßgabe des Informationsfreiheitsgesetzes gegenüber den Behörden des Bundes einen Anspruch auf Zugang zu amtlichen Informationen. Dem Anspruch auf Informationszugang stehen jedoch die Ausschlussgründe des § 3 Nr. 1 c) und § 3 Nr. 2 IFG entgegen.

Im Einzelnen:

A) Zu Ihren Ziffern 1), 2) und 3) a)

Mit Ihren Anträgen 1), 2) und 3) a) begehren Sie:

> *„1) Angabe dahingehend, ob, welche und zu welchem Zweck personendatenverarbeitende Dienste von Organisationen mit Sitz abseits der EU/EWR durch das Bundesministerium für Ernährung und Landwirtschaft eingesetzt werden.*
> *2) Angabe dahingehend, ob, welche und zu welchem Zweck personendatenverarbeitende Dienste von Organisationen mit Sitz innerhalb der EU/EWR, jedoch mit Sub-Auftragnehmern abseits der EU/EWR, durch das Bundesministerium für Ernährung und Landwirtschaft eingesetzt werden.*
> *3) Je einzelnem dieser Dienste mit den vorgenannten Drittlandsbezügen:*
> *a) Ich bitte um eine Angabe dahingehend, ob und welche Übermittlungen nach Art. 44 ff. DSGVO durch die Nutzung dieser Dienste ausgelöst werden."*

Die Herausgabe der von Ihnen mit Ihren Anträgen 1), 2) und 3) a) geforderten Informationen wird nach § 3 Nr. 1 c) und § 3 Nr. 2 IFG abgelehnt. Danach besteht der Anspruch auf Informationszugang nicht, wenn das Bekanntwerden der Information nachteilige Auswirkungen haben kann auf Belange der inneren oder äußeren Sicherheit oder wenn das Bekanntwerden der Informationen die öffentliche Sicherheit gefährden kann.

(1) Ausschlussgrund § 3 Nr. 1 c) IFG

Mit den Belangen der inneren und äußeren Sicherheit schützt § 3 Nr. 1 c) IFG die freiheitlich demokratische Grundordnung sowie den Bestand und die Sicherheit des Bundes und der Länder, einschließlich der Funktionsfähigkeit des Staates und seiner Einrichtungen, vor Angriffen durch fremde Staaten (äußere Sicherheit) oder gewaltsame Aktionen Privater (innere Sicherheit; VG Berlin, Urt. v. 10.2.2011 – 2 K 23/10; vgl. Rossi, IFG, 1. Aufl. 2006, Rn. 16 zu § 3; Schoch, a.a.O., Rn. 33 f. zu § 3). Schutzgut des § 3 Nr. 1 c) IFG ist damit, die Fähigkeit der Bundesrepublik Deutschland, sich nach innen und außen gegen Störungen, die die innere bzw.

äußere Sicherheit beeinträchtigen, zur Wehr setzen zu können (Schoch, IFG, 2. Aufl. 2016, Rn. 55-60 zu § 3). Unter Angriffe auf die innere Sicherheit fallen beispielsweise auch mögliche Anschläge von Terroristen auf Infrastruktureinrichtungen des Bundes (VG Berlin, Urt. v. 10.2.2011 – 2 K 23/10). Nach § 3 Nr. 1 c) IFG ist der Anspruch auf Informationszugang ausgeschlossen, wenn das Bekanntwerden der Information nachteilige Auswirkungen auf das Schutzgut haben „kann". Was den Grad der Gewissheit anlangt, lässt die Vorschrift damit die Möglichkeit nachteiliger Auswirkungen ausreichen (VG Berlin, Urt. v. 10.2.2011 – 2 K 23/10).

Das BMEL ist als oberste Bundesbehörde eine staatliche Einrichtung. Neben der Zuständigkeit für die grundlegenden Themen Ernährung und Landwirtschaft einschließlich des Krisenmanagements ist das BMEL im Rahmen der sog. Kritis-Strategie der Bundesregierung auch zuständig für die kritische Infrastruktur Ernährung. Die sichere Bereitstellung der Dienstleistungen kritischer Infrastrukturen, zu denen unter anderem die Versorgung mit Strom, Wasser, Lebensmitteln und Kommunikation zählen, ist Grundvoraussetzung für die Versorgung der Bevölkerung sowie das Funktionieren von Staat, Wirtschaft und Gesellschaft und damit auch Schutzgut im Sinne des § 3 Nr. 1 c) IFG. Die Koordinierung des Krisenmanagements im Bereich Ernährung und Landwirtschaft erfolgt IT-basiert.

Aus dem Bundeslagebild 2020 des Bundeskriminalamts zum Bereich Cybercrime ergibt sich, dass Angriffe auf Akteure, die für Krisenbewältigung relevant sind, infolge ihrer Bedeutung für Politik, Gesellschaft und Wirtschaft vermehrt stattfinden; das Gefährdungspotenzial, welches von Cyberangriffen ausgeht, ist weiterhin auf einem hohen Niveau (vgl. Bundeslagebild Cybercrime 2020 des Bundeskriminalamts). Das Bundesamt für Sicherheit in der Informationstechnik bewertet die IT-Sicherheitslage in Deutschland in 2020/2021 als angespannt bis kritisch (Die Lage der IT-Sicherheit in Deutschland 2021, BSI, Stand September 2021). Die Situation hat durch den Krieg Russlands gegen die Ukraine eine weitere Verschärfung erfahren. Angesichts der zunehmenden Digitalisierung der öffentlichen Verwaltung stellen Cyberangriffe auf staatliche Institutionen – neben den Gefährdungen durch eine Ausspähung sensibler Daten – eine elementare Gefahr für die Funktionsfähigkeit und Integrität der staatlichen Leistungserbringung dar (Cybersicherheitsstrategie der Bundesregierung aus Sept. 2021). Kritische Infrastrukturen sind für die Versorgung essenziell. Ein Ausfall führt zu großer Verunsicherung und liegt somit im potentiellen Fokus eines möglichen Angreifers.

Aufgrund der zu verzeichnenden deutlichen Zunahme von Cyberangriffen auf staatliche und private Institutionen (vgl. Cybersicherheitsstrategie der Bundesregierung aus Sept. 2021) ist es zwingend erforderlich, potentielle Einfallstore für unberechtigte Dritte weitestgehend zu reduzieren. Auch das BMEL wird regelmäßig Ziel von cyberkriminellen Aktivitäten. Das BMEL verarbeitet im Rahmen seiner Zuständigkeit Daten, die für die Aufrechterhaltung der Staats- und Regierungsfunktionen zum Schutz der Bevölkerung notwendig sind. Das Bekanntwerden der erfragten Informationen, ob, welche, zu welchem Zweck und in welcher Weise

personendatenverarbeitende Dienste genutzt werden, kann die Planung und Durchführung gezielter Cyberangriffe auf die oder mithilfe der vom BMEL genutzten IT-Dienste durch unberechtigte Dritte erleichtern und so die Funktionsfähigkeit der IT-Infrastruktur des BMEL nachhaltig schädigen. Es könnte versucht werden, gezielt in diese Systeme einzudringen, deren Schwachstellen auszunutzen und diese zu kompromittieren. Dabei gilt, je mehr Informationen dem Angreifer zur Verfügung stehen, desto wirksamer und einfacher können Angriffe durchgeführt werden. Eine Störung oder auch ein Ausfall durch einen IT-Sicherheitsvorfall kann die Krisenreaktionsfähigkeit des BMEL stören oder gar ganz ausschalten. Dies wiederum kann zu erheblichen Beeinträchtigungen der öffentlichen Sicherheit und Ordnung führen. Zur Aufrechterhaltung der Funktionsfähigkeit des BMEL ist daher auch eine effektive Absicherung der Informationstechnik notwendig.

Zudem können durch die Offenlegung der erfragten personendatenverarbeitenden Dienste Rückschlüsse auf mögliche Schwerpunktsetzungen im Hinblick auf die Sicherstellung der Staats- und Regierungsfunktionen des BMEL erkennbar werden. Diese Kenntnisse können wiederum von potentiellen Angreifern – auch auf mögliche Schwachstellen hin - untersucht und nutzbar gemacht werden. Das Bekanntwerden der beantragten Informationen kann somit nachteilige Auswirkungen auf Belange der inneren Sicherheit haben. Aufgrund der - zumindest abstrakt - vorhandenen terroristischen und im Zuge des Krieges in der Ukraine konkreter werdenden Bedrohung ist möglichen Angriffen auf wichtige Elemente der Staats- und Regierungsfunktionen im Interesse aller Bürgerinnen und Bürger von vornherein zu begegnen.

(2) Ausschlussgrund § 3 Nr. 2 IFG

Darüber hinaus besteht der Anspruch auf Informationszugang nicht, da das Bekanntwerden der erfragten Informationen die öffentliche Sicherheit gefährden kann, § 3 Nr. 2 IFG. Schutzgut der öffentlichen Sicherheit sind neben den Rechtsgütern des Einzelnen und der Unversehrtheit der Rechtsordnung auch die grundlegenden Einrichtungen und Veranstaltungen des Staates. Darunter fällt auch die Funktionsfähigkeit der staatlichen Einrichtungen (BVerwG, Urteil vom 20.10.2016 – 7 C 20/15 –, juris; OVG Münster, Urt. v. 16.6.2015 – 8 A 2429/14; vgl. BT-Drs. 14/4493, S. 10). Der Ausschlussgrund des § 3 Nr. 2 IFG greift bereits bei einer möglichen konkreten Gefährdung des Schutzguts (OVG Münster, Urt. v. 16.6.2015 – 8 A 2429/14; VG Berlin, Urt. v. 16.7.2015 – 2 K 282/12 – juris Rn. 29 = BeckRS 2015, 50332; VG Köln, ZUM 2013, 906 (907). An die Gefahrenschwelle werden keine strengeren Anforderungen gestellt als im Rahmen des § 3 Nr. 1 IFG, der die Möglichkeit „nachteiliger Auswirkungen“ auf das Schutzgut ausreichen lässt (Vgl. BT-Drs. 15/5606, S. 5 (einheitlicher Schutzstandard); OVG Münster, Urt. v. 16.6.2015 – 8 A 2429/14). Nachteilige Auswirkungen in diesem Sinne liegen vor, wenn aufgrund einer auf konkreten Tatsachen beruhenden prognostischen Bewertung mit hinreichender Wahrscheinlichkeit zu erwarten ist, dass das Bekanntwerden der Information das Schutzgut beeinträchtigt (Vgl. BVerwG, Urteil vom 27. November 2014 - 7 C 18.12 -, ZIP 2015, 496, juris, Rn. 16 ff.; OVG Münster Urt. v. 16.6.2015 – 8 A 2429/14).

Das BMEL ist eine staatliche Einrichtung und fällt somit mit seiner Funktionsfähigkeit unter die Schutzgüter des § 3 Nr. 2 IFG. Das Bekanntwerden der erfragten Informationen kann das Schutzgut auch gefährden. Das BMEL ist regelmäßig Ziel von cyberkriminellen Aktivitäten. Wie bereits dargestellt bestätigt das Bundeskriminalamt, dass Angriffe auf Staats- und Regierungsfunktionen bereits seit 2015 (Deutscher Bundestag) und seit 2020 vermehrt stattfinden. Nachhaltigkeit und Zielauswahl von Cyberangriffen zeigen deutlich den Versuch, die Organe des Bundes, insbesondere die Bundesverwaltung strategisch auszuspionieren. Es ist daher davon auszugehen, dass bei Offenlegung der Informationen diese von Dritten gezielt zu weitergehenden cyberkriminellen Aktivitäten gegenüber dem BMEL ausgewertet und genutzt würden. Damit ist es im Sinne des § 3 Nr. 2 IFG hinreichend wahrscheinlich, dass ein Bekanntwerden der von Ihnen erfragten Informationen die Funktionsfähigkeit des BMEL in seinen für den Bevölkerungsschutz wichtigen Staats- und Regierungsfunktionen beeinträchtigen wird und damit die öffentliche Sicherheit gefährdet wäre. Die Bekanntgabe der erfragten Informationen ist daher nach § 3 Nr. 2 IFG zu versagen.

Der Anspruch auf Informationen dahingehend, ob, welche und zu welchem Zweck personendatenverarbeitende Dienste von Organisationen mit Sitz abseits der EU/EWR bzw. von Organisationen mit Sitz innerhalb der EU/EWR, jedoch mit Sub-Auftragnehmern abseits der EU/EWR durch das BMEL eingesetzt werden, ist demnach genauso nach § 3 Nr. 1 c) und § 3 Nr. 2 IFG zu versagen wie die Angabe dahingehend, ob und welche Übermittlungen nach Art. 44 ff. DSGVO durch die Nutzung dieser Dienste ausgelöst werden.

B) Zu Ihren Ziffern 3) b) und c)

Mit Ihren Anträgen 3) b) und c) begehren Sie:

> *„3) Je einzelnem dieser Dienste mit den vorgenannten Drittlandsbezügen:*
> *b) Ich bitte um sämtliche mit den Anbietern dieser Dienste diesbezüglich abgeschlossenen, datenschutzrechtlich notwendigen Verträge bzw. Fehlanzeige, sollte es keine derartigen Verträge geben. Insbesondere namentlich: Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO sowie Standarddatenschutzklauseln nach Art. 46 DSGVO.*
> *c) Ich bitte um die Bereitstellung des nach Klausel 14 der aktuellen Standarddatenschutz-Klausel-Sets der EU-Kommission bzw. des nach Art. 46 Abs. 1 DSGVO i.V.m. den Grundsätzen aus EuGH-Urteil "Schrems II" notwendigen dokumentierten "Transfer Impact Assessment" bezüglich der mit der Nutzung solcher Dienste einhergehenden Datenübermittlungen.“*

Auch dem Informationsbegehren in Ihren Anträgen 3) b) und c) stehen die Ausschlussgründe § 3 Nr. 1 c) und § 3 Nr. 2 IFG entgegen. Das Bekanntwerden der geforderten Informationen kann nachteilige Auswirkungen haben auf Belange der inneren und äußeren Sicherheit und die öffentliche Sicherheit gefährden.

Die Auskunft darüber, ob solche Verträge bestehen, kann für mögliche Angreifer das Ziel des Angriffes identifizieren.

Zudem werden in Auftragsverarbeitungsverträgen und auch Standardvertragsklauseln u.a. technische und organisatorische Maßnahmen beschrieben, mit denen Datenverarbeitungen abgesichert werden. Es handelt sich dabei um Vereinbarungen zwischen dem Verantwortlichen und dem Auftragsverarbeiter, welche Maßnahmen zu ergreifen sind, um ein dem für die Datenverarbeitung prognostizierten Risiko angemessenes Schutzniveau zu gewährleisten. Diese können Informationen zur Struktur und Absicherung informationstechnischer Systeme bis hin zu organisatorischen Sicherheitsmaßnahmen wie Alarmsysteme für Brand- und Einbruchsfälle umfassen. Dokumentierte „Transfer Impact Assessments“ umfassen u.a. Angaben zu allen relevanten vertraglichen, technischen oder organisatorischen Garantien, die zur Ergänzung der Garantien gemäß den Standardvertragsklauseln eingerichtet wurden, einschließlich Maßnahmen, die während der Übermittlung und bei der Verarbeitung personenbezogener Daten im Bestimmungsland angewandt werden.

Wie bereits dargestellt ist das Gefährdungspotenzial, welches von Cyberangriffen ausgeht, weiterhin auf einem hohen Niveau. Angriffe auf Staats- und Regierungsfunktionen finden vermehrt statt. Cyberkriminelle Aktivitäten richten sich regelmäßig auch gegen das BMEL. Die Absicherung der Verarbeitung personenbezogener Daten durch technische und organisatorische Maßnahmen ist daher ebenso essentiell wie sensibel. Die technischen und organisatorischen Maßnahmen sind wesentlicher Bestandteil zum Schutz auch der IT-Infrastruktur des BMEL. Durch das Bekanntwerden dieser Informationen könnten im ungünstigen Fall durch Manipulation eine erhebliche Schwächung der IT-Infrastruktur des BMEL, mit den unter Punkt A) (1) beschriebenen Folgen für die innere und öffentliche Sicherheit verursacht werden. Das eingerichtete Schutzniveau kann nur beibehalten werden, wenn Informationen über ergriffene technische und organisatorische Maßnahmen zur Sicherung von Datenverarbeitungen nicht bekannt gegeben werden. Nur so kann verhindert werden, dass unberechtigte Dritte die technischen und organisatorischen Maßnahmen auswerten, überwinden und so Zugang zu sensiblen (informationstechnischen) Daten und Systemen erhalten. Ein Bekanntwerden der geforderten Informationen würde das eingerichtete Schutzniveau also in erheblichem Ausmaß abschwächen und damit das Schutzgut der Funktionsfähigkeit des BMEL als staatlicher Einrichtung beeinträchtigen.

Selbst wenn solche Abreden bestünden, würde auf Grund der Standardvertragsklauseln der Europäischen Kommission (Klausel 14 lit. d Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679) für solche Verträge das Interesse des Verantwortlichen und des Auftragsverarbeiters an der Geheimhaltung entsprechender Informationen ebenfalls anerkannt. Denn danach vereinbaren die Parteien standardmäßig lediglich, „Transfer Impact Assessments“ zu dokumentieren und sie der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen. Ein Einsichtsrecht für Jedermann ist nicht vorgesehen.

Damit ist auch der Anspruch auf Zugang zu den in Ihren Anträgen 3) b) und c) erfragten Informationen nach § 3 Nr. 1 c) und § 3 Nr. 2 IFG ausgeschlossen.

Zu II.

Die Kostenentscheidung beruht auf § 10 IFG in Verbindung mit § 1 Absatz 1 der Verordnung über die Gebühren und Auslagen nach dem IFG (Informationsgebührenverordnung – IFGGebV).

Rechtsbehelfsbelehrung
Gegen diesen Bescheid kann innerhalb eines Monats nach Bekanntgabe Widerspruch beim Bundesministerium für Ernährung und Landwirtschaft, Rochusstraße 1, 53123 Bonn erhoben werden.

Mit freundlichen Grüßen
im Auftrag

gez.
[redacted]

*Dieses Dokument wurde elektronisch versandt und ist nur im Entwurf gezeichnet.*