Von: [redacted] [redacted] [[redacted]bsi.bund.de]
Gesendet: Mittwoch, 31. August 2022 08:03
An: Referat 25 Postfach
Cc: GP Referat BL 24; GP Datenschutzbeauftragte
Betreff: AW: Bitte um Stellungnahme zu festgestellten Datenschutzverstößen

Az.: 25-170 II#1143

Sehr geehrter [redacted],

ich nehme Bezug auf Ihre E-Mail vom 28. Juni 2022 wegen des Auskunftsersuchens nach Art. 15 DSGVO, das Herr Joachim Lindenberg am 22.03.2022 an das BSI gerichtet hatte (unser Zeichen: BL24-010 03 02/2022-006).

Gerne möchte ich Ihre Fragen dazu beantworten:
(a) Plant das BSI Maßnahmen, um dem Petenten die Ausübung seiner Rechte zu ermöglichen (Vervollständigung der Auskunft, formgerechte Zustellung, korrekte Datenschutzerklärung)?
Ja, wir haben zwischenzeitlich eine umfassendere Antwort an den Betroffenen vorbereitet, welche alle in unserem Haus vorhandene Datenkopien und eine angepasste Datenschutzerklärung umfasst.
Wir stehen derzeit im Austausch mit dem Betroffenen, um abzuklären, in welcher (elektronischen) Form die Dokumente übersandt werden können, bspw. per verschlüsselter E-Mail oder USB-Stick.

(b) Plant das BSI Maßnahmen, die sicherstellen, dass sich die o.g. Verstöße zukünftig nicht mehr wiederholen, z.B. durch die Implementierung eines DSGVO-konformen Standardprozesses zur Bearbeitung von Auskunftsersuchen nach Art. 15 DSGVO?
- Abfrage Prozess im BSI

In unserer Stellungnahme vom 4. Mai 2022 haben wir zusammenfassend dargelegt, wie der BSI-interne Prozess zur Bearbeitung von Betroffenenanfragen nach der DSGVO ausgestaltet ist. Dieser sieht aktuell nicht vor, Auskunftsanfragen nach Art. 15 DSGVO an sämtliche Organisationseinheiten (OE) auszusteuern. Nachfolgend legen wir ergänzend zu den Erläuterungen in o.g. Stellungnahme dar, aufgrund welcher Kriterien die Auswahl der im BSI abgefragten OE getroffen wurde. Ziel unseres aktuellen Prozesses ist eine transparente Identifizierung aller Informationen für den Betroffenen im BSI mit hoher Detailtiefe unter Beibehaltung eines zweckgerichteten und effektiven Verwaltungshandelns.
1) Kriterium: Es werden nur so viele OE abgefragt wie unbedingt nötig.
Wir versuchen damit, im Sinne der Datensparsamkeit gem. Art. 5 Abs. 1 lit. c DSGVO, aktiv zu verhindern, dass personenbezogene Daten eines Betroffenen im BSI nur durch seine Anfrage selbst verbreitet und damit verarbeitet werden, ohne dass dies nötig ist.
2) Kriterium: Aufgrund der Zweckbindung von personenbezogenen Daten werden OE entsprechend ihrer Aufgaben, ihrem Außenkontakt und des Verzeichnisses von Verarbeitungstätigkeiten abgefragt, um die sachliche Richtigkeit der Daten zu gewährleisten.
Derzeit werden sämtliche OE per E-Mail abgefragt, die aufgrund ihrer Aufgaben und des Verzeichnisses von Verarbeitungstätigkeiten Kontakt zu externen Personen haben (z.B. Personalgewinnung, Kontakt zu Bürgern, Organisation von Veranstaltungen, Verwaltung von Meldeportalen, Bearbeiten von Anfragen unterschiedlicher Art, Detektion/Reaktion von Cyberangriffen etc.). Im Regelfall können nur bei diesen OE personenbezogene Daten externer Personen verarbeitet werden. Im Detail bedeutet dies, dass wir insbesondere Organisationseinheiten abgefragt haben, die folgende Aufgaben erfüllen:
- Öffentlichkeitsarbeit, Verbraucherschutz, Cybersicherheit für Bürger und Gesellschaft

- Personalabteilung
- CERT Bund
- OE, die Anfragen unterschiedlicher Art beantworten (IFG, Bürgeranfragen, etc.)
- OE mit (externer) Beratungsfunktion
- OE, die zur Aufgabenerfüllung Kontakte pflegen müssen
- OE, deren Aufgabe u.a. die Betreuung von Studierenden ist
- OE, deren Aufgaben u.a. Zertifizierung oder Zulassung sind
- OE, deren Aufgabe die Vorfallsbearbeitung ist
- OE, die mit Herstellern, Wirtschaftsunternehmen, Verbänden, Betreibern des Internets, Anbietern von Internetanwendungen / Software-Komponenten / Telemediendiensten o.ä. zusammenarbeiten
- OE, die in Gremien / Verbänden / Stiftungen tätig sind
- OE, die mit Forschungsstellen oder anderen externen Stellen zusammenarbeiten
- OE, die für Penetrationstests zuständig sind, Lagezentrum
- OE, die eine Kontaktdatenbank pflegen
- OE für Vergabe und Projekte, Haushalt

Die Abfrage findet aktuell per E-Mail statt, was, insbesondere im Falle einer Fehlanzeige, die personenbezogenen Daten eines Betroffenen innerhalb des BSI weiterverstreut. Dem möchten wir entgegenwirken und haben deshalb OE ohne Kontakt zu externen Personen bei einer Betroffenenanfrage durch einen Externen im Standardprozess zunächst ausgeschlossen.
Dieser Ausschluss findet jedoch nicht ohne Prüfung im Einzelfall statt: Erreicht das BSI ein Auskunftsbegehren eines externen Betroffenen und lässt das Begehren nach Prüfung darauf schließen, dass auch noch andere (oben nicht aufgeführte) OE im BSI betroffen sein könnten, werden diese selbstverständlich in der Abfrage berücksichtigt.
Da unter den oben genannten Parametern eine umfassende Abfrage im BSI stattgefunden hat, möchten wir um eine neue Bewertung der Rechtmäßigkeit unseres Vorgehens bitten.

Zukünftig planen wir, die Abfrage nicht mehr per E-Mail im BSI zu verteilen, sondern dies innerhalb einer Software abzubilden. Wir befinden uns derzeit in der Testphase unseres neuen Datenschutzmanagement Tools Otris und hoffen, eine Hausabfrage innerhalb des Tools vornehmen zu können. Dies wäre wesentlich datensparsamer, als eine Abfrage per E-Mail, weshalb in einem solchen Fall problemlos alle OE im BSI beteiligt werden könnten.

- Herausgabe von Datenkopien nach Art. 15 Abs. 3 DSGVO

Bisweilen hat das BSI Betroffenen Datenkopien nur auf Antrag, nach Art. 15 Abs. 3 DSGVO, zur Verfügung gestellt.
Den Antrag des Herrn Lindenberg haben wir analog §§ 133, 157 BGB dahingehend ausgelegt, dass dieser eine Bestätigung darüber verlangte, ob ihn betreffende personenbezogene Daten im BSI verarbeitet werden, Art. 15 Abs. 1 DSGVO. Aufgrund des kombinierten Antrags aus Art. 15 DSGVO sowie § 29 VwVfG erstreckte sich der Wille des Betroffenen im Rahmen des Auskunftsanspruches nach unserer Auffassung nicht auch zusätzlich auf die Herausgabe der Datenkopien, da ansonsten der Anspruch aus § 29 VwVfG auf Akteneinsicht ins Leere gelaufen wäre. Eine solche Bestätigung und Übersicht zu den durch das BSI verarbeiteten personenbezogenen Daten wurden sodann fristgerecht zur Verfügung gestellt.
Entsprechend Ihrer Auslegung des Auskunftsbegehrens vom 22.03.2022 haben wir die Bereitstellung der Datenkopien nachgeholt und werden diese dem Betroffenen nach Abstimmung eines sicheren Übertragungsweges (elektronisch) zukommen lassen.
Uns ist bewusst, dass es sich bei der Auslegung des Art. 15 DSGVO und vor allem die Abgrenzung des Abs. 1 zum Abs. 3 um ein hochumstrittenes Thema handelt, welches noch nicht höchstrichterlich entschieden

wurde. Wir würden uns über einen inhaltlichen Austausch zur Umsetzung des Art. 15 Abs. 3 DSGVO mit Ihnen sehr freuen, um herausfinden zu können, wie genau Sie eine Abgrenzung vornehmen und in welchen Fällen und in welchem Umfang Ihrer Ansicht nach tatsächlich Datenkopien herauszugeben sind.
Gerne würden wir dazu einen Termin, beispielsweise in Form einer Videokonferenz mit Ihnen vereinbaren. Für Terminvorschläge ab 4.Oktober 2022 sind wir offen.

Für telefonische Rückfragen stehen wir jederzeit zur Verfügung.

Viele Grüße

[redacted]

Referat BL 24 - Rechtliche Begleitung der Verwaltungsverfahren
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185 - 189
53175 Bonn
Telefon: +49 228 99 9582-[redacted]
Mobil: +49 [redacted]
E-Mail: [redacted]bsi.bund.de
Internet: www.bsi.bund.de

#DeutschlandDigitalSicherBSI

Alle Informationen zum Umgang mit Ihren personenbezogenen Daten finden Sie unter
www.bsi.bund.de/datenschutz

-----Ursprüngliche Nachricht-----
Von: [redacted] <[redacted]@bfdi.bund.de> Im Auftrag von Referat 25 Postfach
Gesendet: Freitag, 29. Juli 2022 11:07
An: [redacted] <[redacted]bsi.bund.de>
Cc: GP Referat BL 24 <referat-bl24@bsi.bund.de>; GP Datenschutzbeauftragte <datenschutzbeauftragte@bsi.bund.de>
Betreff: AW: Bitte um Stellungnahme zu festgestellten Datenschutzverstößen

Liebe Frau [redacted]

eine Fristverlängerung bis zum 31.08.2022 ist aus unserer Sicht möglich. Ich bitte Sie daher um Rückmeldung bis zum 31.08.2022.

Leider hatte ich Ihre Nummer nicht auf meinem Display, werde Sie aber im Laufe des Vormittags noch anrufen.

Mit freundlichen Grüßen

[redacted]

****
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Referat 25
Graurheindorfer Straße 153, 53117 Bonn
Fon: (0228) 997799-[redacted]
Fax: (0228) 99107799-[redacted]
E-Mail: referat25@bfdi.bund.de
Internet: https://www.bfdi.bund.de
****
Datenschutzrechtliche Erklärung des BfDI für den E-Mail-Verkehr und die Erfüllung seiner öffentlichen Aufgaben insgesamt: (nachstehender Link führt auf den Internetauftritt des BfDI unter www.bfdi.bund.de)

https://www.bfdi.bund.de/datenschutz

****
Hinweis: Dies ist eine vertrauliche Nachricht und nur für den Adressaten bestimmt. Sollten Sie irrtümlich diese Nachricht erhalten haben, informieren Sie bitte sofort den Absender und vernichten Sie diese E-Mail.

****
Privacy statement of the BfDI for correspondence by email and for managing its overall public responsibility: (the following link is directing to the web presence of the BfDI at www.bfdi.bund.de)

https://www.bfdi.bund.de/EN/Service/PrivacyStatement/PrivacyStatement-node.html

****
Confidentiality notice: This is a confidential message and it is intended only for the addressee. If you have received this message by mistake, please immediately inform the sender and destroy this email.

-----Ursprüngliche Nachricht-----
Von: [redacted] [mailto:[redacted]bsi.bund.de]
Gesendet: Freitag, 29. Juli 2022 10:52
An: [redacted] <[redacted]@bfdi.bund.de>
Cc: GP Referat BL 24 <referat-bl24@bsi.bund.de>; Referat 25 Postfach <REFERAT25@bfdi.bund.de>; GP Datenschutzbeauftragte <datenschutzbeauftragte@bsi.bund.de>
Betreff: AW: Bitte um Stellungnahme zu festgestellten Datenschutzverstößen

Lieber [redacted],

da ich Sie in den vergangenen Tagen telefonisch nicht erreichen konnte, möchte ich Sie gerne auf diesem Wege um eine Verlängerung der Frist zur Rückantwort um vier Wochen bitten.

Hintergrund ist, dass wir Ihre Nachricht zum Anlass genommen haben, unsere internen Prozesse nochmals gänzlich zu überprüfen und anzupassen und sich dies, während urlaubs- und krankheitsbedingten Abwesenheiten, nicht schneller umsetzen lässt.

Ich bedanke mich im Voraus und stehe Ihnen selbstverständlich für Rückfragen zur Verfügung.

Viele Grüße

[redacted]

Referat BL 24 - Rechtliche Begleitung der Verwaltungsverfahren
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185 - 189
53175 Bonn
Telefon: +49 228 99 9582-[redacted]
Mobil: +49 [redacted]
E-Mail: [redacted]bsi.bund.de
Internet: www.bsi.bund.de

#DeutschlandDigitalSicherBSI

Alle Informationen zum Umgang mit Ihren personenbezogenen Daten finden Sie unter www.bsi.bund.de/datenschutz

-----Ursprüngliche Nachricht-----
Von: [redacted] <[redacted]@bfdi.bund.de> Im Auftrag von Referat 25 Postfach
Gesendet: Dienstag, 28. Juni 2022 12:11
An: GP Datenschutzbeauftragte <datenschutzbeauftragte@bsi.bund.de>
Cc: Referat 25 Postfach <REFERAT25@bfdi.bund.de>; GP Geschaeftszimmer_BL <geschaeftszimmer-bl@bsi.bund.de>
Betreff: Bitte um Stellungnahme zu festgestellten Datenschutzverstößen

Der Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit (BfDI)

Az.: 25-170 II#1143

Sehr geehrte Damen und Herren,

wie heute Vormittag mit Herrn [redacted] besprochen, melde ich mich wegen des Auskunftsersuchens nach Art. 15 DSGVO, das Herr Joachim Lindenberg am 22.03.2022 an Ihr Haus gerichtet hatte (Ihr Zeichen: BL24-010 03 02/2022-006).

Im Rahmen unserer Sachverhaltsermittlung und -bewertung wurden folgende DSGVO-Verstöße des BSI im Kontext des o.a. Auskunftsersuchens festgestellt:

(1) Unvollständige Auskunft
Nach hiesiger Kenntnis existierten zum Zeitpunkt der Beantwortung des Auskunftsersuchens zehn offene Vorgänge beim BSI, bei denen jeweils personenbezogene Daten von Herrn Lindenberg verarbeitet wurden (vgl. hier, ganz unten: https://blog.lindenberg.one/BundesamtUnsicherheit). Da der Petent in seinem Auskunftsersuchen um eine "vollständige Auskunft nach Art. 15 DSGVO" gebeten hatte, hätten ihm aus hiesiger Sicht im Kontext des Art. 15 Abs. 1 und 3 DSGVO i.V.m. Art. 4 Abs. 1 Nr. 1 DSGVO all diese Verarbeitungen kommuniziert und als Kopie zur Verfügung gestellt werden müssen. Dies ist jedoch nicht erfolgt, womit dem Petenten sein Auskunftsrecht nach Art. 15 DSGVO nicht vollumfänglich gewährt wurde.
Nach der Sachverhaltsermittlung durch den BfDI ergibt sich weiterhin folgendes Bild: Bei Eingang eines Auskunftsersuchens nach Art. 15 DSGVO erfolgt beim BSI bisher keine Abfrage aller Organisationseinheiten, ob personenbezogene Daten zum Antragstellenden vorliegen. Es werden lediglich einige ausgewählte Organisationseinheiten abgefragt, namentlich diejenigen, die üblicherweise "Außenkontakt" haben (siehe Stellungnahme des BSI vom 04.05.2022). So ist aus hiesiger Sicht auch die unvollständige Auskunft an den Petenten zu erklären.

(2) Keine formgerechte Zustellung
Eine Kopie der verarbeiteten personenbezogenen Daten ist der betroffenen Person gemäß Art. 15 Abs. 3 S. 3 DSGVO in einem "gängigen elektronischen Format" zur Verfügung zu stellen, sofern diese ihren Antrag elektronisch stellt. Vorliegend wurden die Kopien aber trotz elektronischer Antragstellung in Papierform übermittelt (Anmerkung: Es geht hier nicht um das Schreiben an den Petenten, sondern um die darin enthaltenen Kopien personenbezogener Daten nach Art. 15 Abs. 3 DSGVO).

(3) Angaben zu Löschfristen
Die Angaben zu den Löschfristen (vgl. Ziffer 3.c) der "Datenschutzrechtliche[n] Hinweise" im Antwortschreiben des BSI vom 11.04.2022) sind aus hiesiger Sicht nicht mehr aktuell, da sie die Überarbeitung des § 5 BSIG nicht berücksichtigen. Laut § 5 BSIG sind personenbezogene Daten unverzüglich bzw. bei Vorliegen bestimmter Voraussetzungen spätestens nach 18 Monaten zu löschen. In Ziffer 3.c) der "Datenschutzrechtliche[n] Hinweise" ist jedoch von einer Speicherdauer von "maximal drei Monaten" die Rede.

Im Kontext dieser Verstöße möchte ich Sie um folgende Auskünfte bitten:

(a) Plant das BSI Maßnahmen, um dem Petenten die Ausübung seiner Rechte zu ermöglichen (Vervollständigung der Auskunft, formgerechte Zustellung, korrekte Datenschutzerklärung)?
(b) Plant das BSI Maßnahmen, die sicherstellen, dass sich die o.g. Verstöße zukünftig nicht mehr wiederholen, z.B. durch die Implementierung eines DSGVO-konformen Standardprozesses zur Bearbeitung von Auskunftsersuchen nach Art. 15 DSGVO?

Für eine Rückantwort bis zum 29.07.2022 wäre ich Ihnen dankbar.

Für telefonische Rückfragen stehe ich ebenfalls gerne zur Verfügung.

Mit freundlichen Grüßen
[redacted]

****
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Referat 25
Graurheindorfer Straße 153, 53117 Bonn
Fon: (0228) 997799-[redacted]
Fax: (0228) 99107799-[redacted]
E-Mail: referat25@bfdi.bund.de
Internet: https://www.bfdi.bund.de
****
Datenschutzrechtliche Erklärung des BfDI für den E-Mail-Verkehr und die Erfüllung seiner öffentlichen Aufgaben insgesamt: (nachstehender Link führt auf den Internetauftritt des BfDI unter www.bfdi.bund.de)

https://www.bfdi.bund.de/datenschutz

****

****
Privacy statement of the BfDI for correspondence by email and for managing its overall public responsibility: (the following link is directing to the web presence of the BfDI at www.bfdi.bund.de)

https://www.bfdi.bund.de/EN/Service/PrivacyStatement/PrivacyStatement-node.html

****