Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

**Prof. Ulrich Kelber**
Bundesbeauftragter
für den Datenschutz und
die Informationsfreiheit

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

Deutscher Bundestag
Ausschuss für Inneres und Heimat
Platz der Republik 1

Per Email an
innenausschuss@bundestag.de

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn

FON (0228) 997799-5000
FAX (0228) 997799-5550

E-MAIL referat23@bfdi.bund.de

INTERNET www.bfdi.bund.de

DATUM Bonn, 18.12.2020
GESCHÄFTSZ. 23-170/024#0877

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

BETREFF **Gesetzentwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme**

Sehr geehrte Frau Ausschussvorsitzende Lindholz,
sehr geehrte Damen und Herren,

der vom Bundesminister des Innern, für Bau und Heimat vorgelegte Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme wurde von der Bundesregierung in der Kabinettsitzung am 16. Dezember 2020 beschlossen.

Anliegend übersende ich Ihnen meine korrespondierende Stellungnahme verbunden mit der Bitte um freundliche Berücksichtigung.

Mit besten Grüßen

[redacted]
Ulrich Kelber



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

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, den 18.12.2020

# Stellungnahme

**des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit**

**zum Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0)**

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

**Cyber- und Informationssicherheit ist wichtiger Vertrauensanker**

Die Digitalisierung durchdringt alle Lebensbereiche. Die Cyber- und Informationssicherheit ist hierbei ein essentieller Vertrauensanker. Digitalisierung, Cybersicherheit und Datenschutz sind untrennbar miteinander verbunden. IT-Sicherheitsvorfälle bedrohen regelmäßig auch die Schutzgüter des Datenschutzes. Das mit der Novelle des IT-Sicherheitsgesetzes verfolgte Ziel eines verbesserten Schutzes von Gesellschaft und Wirtschaft in der digitalen Welt unterstütze ich deshalb nachdrücklich. Hierauf gerichtete Maßnahmen müssen aber in Einklang mit dem Datenschutz stehen.

Das IT-Sicherheitsgesetz 2.0 wird bereits seit geraumer Zeit diskutiert. Ein erster Gesetzentwurf wurde mir bereits im Frühjahr 2019 auf Ressortebene zugeleitet. Ein zweiter Entwurf folgte im Mai 2020. Der dritte Referentenentwurf wurde im November 2020 zirkuliert. Trotz dieses langen Zeitraums waren die Fristen für meine Stellungnahmen stets äußerst ambitioniert bemessen. Im Rahmen dieser schwierigen Bedingungen wurde das Verfahren bestmöglich begleitet. Es fand ein intensiver Austausch auf Ressortebene statt. Viele meiner Kritikpunkte wurden hierbei aufgegriffen und umgesetzt. Diverse ursprünglich geplante, aus meiner Sicht überbordende und deshalb datenschutzrechtlich kritische Neuregelungen u.a. im Straf- und Strafprozessrecht wurden gestrichen, was ich sehr begrüße.

**Keine unangemessene Ausweitung der Speicherdauer von Protokolldaten**

Weiterhin kritisch sehe ich aber insbesondere die in dem Gesetzentwurf in Artikel 1 Nr. 4, § 5 Abs. 2 BSIG-Entwurf (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik) geplante Ausweitung der Speicherung von Protokolldaten von bisher drei auf zwölf Monate.

Meine zugrundeliegenden Bedenken basieren auf folgenden Überlegungen:

Im Gesetzentwurf wird damit argumentiert, diese Ausweitung sei für eine effektive Aufklärung von Cyberangriffen unerlässlich. Denn Cyberangriffe würden sich typischerweise über einen längeren Zeitraum erstrecken und nur mit vorhandenen Protokolldaten sei eine Rekonstruktion des Angriffs und eine bestmögliche Schadensbeseitigung möglich. Die Motivation für die längere Speicherdauer ist nachvollziehbar, rechtfertigt aus meiner Sicht aber nicht ihre erhebliche Ausweitung und wirft Fragen der Verhältnismäßigkeit auf.

Die Speicherung von Protokolldaten für zwölf Monate wird die Regel und nicht die Ausnahme sein. Eine Speicherung von Protokolldaten darf nach dem BSIG bereits heute erfolgen, wenn tatsächliche Anhaltspunkte bestehen, dass die Protokolldaten zur Abwehr einer bereits bestehenden Gefahr erforderlich sein können. Konkret müssen der Norm entsprechend tatsächliche Anhaltspunkte bestehen, „dass diese [Protokolldaten] für den Fall der Bestätigung eines Verdachts nach Absatz 3 Satz 2 [BSIG] zur Abwehr von Gefahren, die von dem gefundenen Schadprogramm ausgehen oder zur Erkennung und Abwehr anderer Schadprogramme erforderlich sein können“. Diese Voraussetzung dürfte stets anzuneh-

men sein, so dass eine Speicherung der Protokolldaten nicht nur Ausnahmecharakter haben dürfte.

Nach der gesetzlichen Definition von Protokolldaten in § 2 Abs. 8 S. 2 BSIG können Protokolldaten Verkehrsdaten enthalten, so dass es sich insoweit um eine „Vorratsdatenspeicherung“ handelt. Eine unterschiedslose Speicherung ohne konkreten Anlass stellt einen besonders schwerwiegenden Eingriff in die Grundrechte der Betroffenen dar, weil kein Zusammenhang zwischen dem Verhalten der Personen, deren Daten betroffen sind, und dem mit der fraglichen Regelung verfolgten Zweck vorliegt.

Generell gilt, dass die Speicherdauer von Protokolldaten auf das zwingend notwendige Maß zu beschränken ist. Das Bundesverfassungsgericht führte hierzu bereits vor einer Dekade in einem Grundsatzurteil zur konkreten Ausgestaltung der Vorratsdatenspeicherung aus, dass eine Speicherungsdauer von sechs Monaten „an der Obergrenze dessen [ist], was unter Verhältnismäßigkeitserwägungen rechtfertigungsfähig ist“, vgl. BVerfG, Urteil des Ersten Senats vom 02. März 2010 - 1 BvR 256/08 -, Rn. 215. Bereits in diesem Lichte begegnet die geplante Ausweitung der Speicherdauer erheblichen rechtlichen Bedenken mit Blick auf ihre Verhältnismäßigkeit.

Die Ausweitung der Speicherdauer zur Stärkung der Cyber-Resilienz der Kommunikationstechnik des Bundes würde zusätzlich aber auch die - bereits heute bestehende - Inkongruenz zum privatwirtschaftlichen Telekommunikationssektor weiter vergrößern. In der Telekommunikationsbranche können Verkehrsdaten z.B. für die Störungserkennung, dem Schutz vor Missbrauch und für die generelle Netzsicherheit genutzt werden, vgl. § 100 Abs. 1 und 3 und § 109 Telekommunikationsgesetz. Hier werde ich (sofern kein konkreter Anlass besteht, etwa eine konkrete Störung) auch weiterhin auf eine maximale Speicherdauer von sieben Tagen bestehen.

Die geplante Ausweitung der Speicherdauer in § 5 Abs. 2 BSIG-Entwurf ist nach alledem abzulehnen.