Stellungnahme

bitkom

zum Regierungsentwurf für ein Hinweisgeberschutzgesetz

1. Ausgangslage

Mit der Richtlinie (EU) 2019/1937 (sog. HinSch-RL) vom 23. Oktober 2019 möchte die EU-Kommission die Durchsetzung des Unionsrechts stärken. Daneben hat die Richtlinie das Ziel, Hinweisgeber zu schützen und ihnen die Angst vor Repressalien zu nehmen. Die Richtlinie war nach Art. 26 Abs. 1 der HinSch-RL bis zum 17. Dezember 2021 umzusetzen. Im Juni 2022 hat das Kabinett den Regierungsentwurf für ein Hinweisgeberschutzgesetz beschlossen. Dieser Regierungsentwurf ist Gegenstand der vorliegenden Stellungnahme.

2. Bewertung des Bitkom

Der Bitkom begrüßt weiterhin grundsätzlich die gut durchdachte Gesetzgebung zur Umsetzung der Hinweisgeberschutz-Richtlinie.

Jedoch ist es an dieser Stelle von besonderer Bedeutung, durch die neuen Regelungen keine weiteren Rechtsunsicherheiten zu provozieren. Insbesondere ist es entsprechend unserem Petitum aus der Stellungnahme zum Referentenentwurf dringend erforderlich, einen stärkeren Gleichlauf mit datenschutzrechtlichen Bestimmungen herzustellen.

Außerdem sollte der Umsetzungsaufwand vor allem für kleinere und mittlere Unternehmen reduziert werden, indem die erforderliche Datenschutz-Folgenabschätzung bereits im Gesetzgebungsverfahren durchgeführt wird.

2.1 Zu § 3 Abs. 8 HinSchG-E

§ 3 Abs. 8 HinSchG-E definiert den Begriff der Beschäftigten. Der Wortlaut dieser Definition ist nicht identisch mit § 26 Abs. 8 BDSG. Hier würden wir einen gleichlautenden Wortlaut oder aber eine gesetzliche Verweisung begrüßen, um Fehlinterpretationen zu vermeiden.

2.2 Zu § 5 Abs. 2 Nr. 3/Nr. 4 HinSchG-E

Die Normen umfassen nicht alle Berufsgruppen des § 203 Abs. 1 StGB, insb. werden Steuerberater und Wirtschaftsprüfer nicht einbezogen und damit nicht vom Anwendungsbereich ausgenommen. Zudem sind Rechtsanwälte nach § 3 Nr. 1 StBerG zur geschäftsmäßigen Hilfeleistung in Steuersachen befugt und es ergäben sich dann eklatante Abgrenzungsfragen in der Praxis bei Personen mit Doppelqualifikationen, wenn eine davon vom Anwendungsbereich ausgenommen wäre. Für Dienstleister dieser Berufsgruppen müsste zudem nach § 5 Abs. 2 Nr. 5 HinSchG-E stets eine Differenzierung bezogen auf einzelne Datensätze durchgeführt werden.

Berlin,
24. August 2022

Bitkom e.V.

Charleen Roloff
Referentin Legal Tech und Recht

T +49 30 27576-199
c.roloff@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

2.3 Zu § 9 Abs. 4 Nr. 1 HinSchG-E

Es sollte geregelt werden, dass sich die Voraussetzungen bzw. Anforderungen an die Einwilligung nach den Vorgaben der DSGVO richten.

2.4 Zu § 10 HinSchG-E

Gemäß § 10 HinSchG-E sind Meldestellen befugt, personenbezogene Daten zu verarbeiten, soweit dies zur Erfüllung ihrer in den §§ 13 und 24 HinSchG-E bezeichneten Aufgaben erforderlich ist. Diese Regelung war bereits genauso im Referentenentwurf vorgesehen.

Es ist nicht verständlich, wieso die in § 11 HinSchG-E enthaltenen Dokumentationspflichten nicht in § 10 HinSchG-E erwähnt werden. Die Dokumentation ist ebenso verpflichtend für Unternehmen im Anwendungsbereich des Entwurfes wie die Erfüllung der in §§ 13 und 24 HinSchG-E genannten Pflichten. Für die Erfüllung der Dokumentationspflichten aus § 11 HinSchG-E sind ebenfalls Verarbeitungen personenbezogener Daten erforderlich. Daher erschließt sich nicht, warum § 10 HinSchG-E nicht auch auf § 11 HinSchG-E verweist. Es sollte ein Verweis auf § 11 HinSchG-E in § 10 HinSchG-E ergänzt werden.

2.5 Zu § 11 Abs. 5 HinSchG-E

Gemäß § 11 Abs. 5 HinSchG-E müssen die dokumentierten Meldungen zwei Jahre nach Abschluss des Verfahrens gelöscht werden. Diese Vorschrift ist aus zwei Gründen problematisch. Einerseits regelt sie eine Löschpflicht und steht dadurch im Konflikt mit den allgemeinen Zulässigkeitsvoraussetzungen des Art. 6 DSGVO und Art. 9 DSGVO. Andererseits ist die Frist so kurz gewählt, dass die nicht im Einklang mit allgemeinen Verjährungsfristen steht.

Die allgemeine Verjährungsfrist aus § 195 BGB beträgt drei Jahre. Wenn Unternehmen allerdings verpflichtet sind, zwei Jahre nach Abschluss des Verfahrens die nach § 8 HinSchG-E erfolgte Dokumentation zu löschen, können diese Unternehmen ggf. auch nicht mehr die notwendigen Nachweise für rechtskonformes Handeln erbringen. Zudem sind in manchen Bereichen auch noch längere Verjährungsfristen denkbar. Die Regelung in § 11 Abs. 5 HinSchG-E sollte daher auf die im deutschen Recht bekannten Verjährungsfristen abgestimmt sein. Zudem sollte klargestellt werden, ab wann das Verfahren im Sinne von § 11 Abs. 5 HinSchG-E abgeschlossen ist und bei Bestimmung dieses Zeitpunktes auch Verjährungsfristen eine Rolle spielen.

Des Weiteren sollte der deutsche Gesetzgeber insgesamt davon absehen, eine Regelung zu erlassen, die im Konflikt mit Art. 6 DSGVO und Art. 9 DSGVO steht. Gemäß diesen beiden Artikeln der DSGVO wird die Rechtmäßigkeit einer Datenverarbeitung und damit auch die Rechtmäßigkeit einer Speicherung und Aufbewahrung von personenbezogenen Daten abschließend geregelt. Der nationale Gesetzgeber muss den Vorrang des Unionsrechts respektieren und darf durch eine Löschpflicht nicht auch ein „Verbot“ einer länger als zwei Jahre andauernden Aufbewahrung in Bezug auf personenbezogene Daten regeln. Für eine über zwei Jahre hinaus gehende Aufbewahrung der Dokumentation müssen in Bezug auf

personenbezogene Daten die allgemeinen Zulässigkeitsvoraussetzungen aus Art. 6 DSGVO und Art. 9 DSGVO gelten. Der HinSchG-E sollte insgesamt keine Löschpflicht regeln, die Bestimmungen der DSGVO berührt.

Darüber hinaus ist zu beachten, dass mitunter auch Syndikusrechtsanwälte oder andere Rechtsanwälte als interne Meldestelle fungieren. Diese sind gemäß § 50 Abs. 1 BRAO dazu verpflichtet, Handakten für sechs Jahre aufzubewahren. Die in § 11 Abs. 5 HinSchG-E vorgeschlagene Löschpflicht, steht ebenfalls im Konflikt mit der Pflicht aus § 50 Abs. 1 BRAO.

Die Bundesregierung könnte diese Konflikte dadurch vermeiden, dass das Gesetz auf bereits bestehende gesetzliche Aufbewahrungspflichten und Löschfristen verweist. Eine starre Frist von 2 Jahren würde nur dann Sinn ergeben, wenn hierdurch ein erhöhter Aufbewahrungsbedarf zur Erbringung von Nachweisen zum Ausdruck gebracht werden würde, indem die 2 Jahre auf die bestehenden gesetzlichen Fristen „obendrauf geschlagen“ werden.

2.6 Zu § 16 Abs. 1 S. 4 HinSchG-E

In der Gesetzesbegründung wird darauf verwiesen, dass *„auch anonyme Meldungen bearbeitet werden sollen“* und dies *„insbesondere bei der Meldung gravierender Verstöße“* gilt. Sofern der Gesetzgeber einen unterschiedlichen Umgang je nach Grad des gemeldeten Verstoßes regeln möchte, so sollte er das im Gesetzestext selbst machen und nicht ausschließlich in der Gesetzesbegründung beiläufig auf die Schwere des Verstoßes abstellen.

2.7 Zu § 17 Abs. 1 S. 4 HinSchG-E

In § 17 Abs. 1 Satz 4 HinSchG-E hat die Bundesregierung gegenüber dem Referentenentwurf einen Zusatz eingefügt. Es soll zwar dabeibleiben, dass interne Meldekanäle nicht für die Entgegennahme anonymer Meldungen ausgelegt sein müssen. Allerdings ist nun vorgesehen, dass *„die interne Meldestelle (...) auch anonym eingehende Meldungen bearbeiten (sollte), soweit dadurch die vorrangige Bearbeitung nichtanonymer Meldungen nicht gefährdet wird.“*

Es drängt sich die Frage auf, wie und in welchen Fällen Unternehmen anonyme Hinweismeldungen überhaupt erhalten können sollen, wenn der Meldekanal so ausgestaltet ist, dass eine anonyme Meldung nicht möglich ist.

Der HinSchG-E stellt für die Pflicht zur Bearbeitung anonymer Meldungen allein auf die Gefährdung der vorrangigen Bearbeitung von nichtanonymen Meldungen ab. Wenngleich die dadurch zum Ausdruck gebrachte Beachtung des Aufwands für sich genommen nicht kritikwürdig ist, so ist ein ausschließliches Abstellen auf den Aufwand jedoch nicht praxisgerecht. Es gibt mehrere Faktoren, die dafür entscheidend sind, ob eine Bearbeitung von anonymen Meldungen sachgerecht und möglich ist. Hierzu zählen mindestens u.a. die folgenden Aspekte:

- Bestehen einer Möglichkeit zur Kontaktaufnahme mit Hinweisgebern, um die Vorgaben zum Verfahren bei internen Meldungen aus § 17 HinSchG-E einzuhalten. Insbesondere die Pflichten aus § 17 Abs. 1 Nr. 1, Nr. 3 und Nr. 5 HinSchG-E sowie die Pflichten aus § 17 Abs. 2 HinSchG-E sind ohne Möglichkeit zur Kontaktaufnahme – die bei anonymen im Gegensatz zu pseudonymen Meldungen in der Regel nicht vorhanden ist – nicht erfüllbar.
- Vorhandensein einer Möglichkeit, die anonyme Meldung ausgewogen und sachgerecht zu bearbeiten, obwohl der anonyme Hinweisgeber – mangels Möglichkeit zur Kontaktaufnahme mit diesem – im weiteren Verfahren keine weiteren Angaben mehr zu seiner Sicht auf den Sachverhalt machen kann.

Insgesamt sollte sich die Bundesregierung bewusst sein, dass anonyme Meldungen in den seltensten Fällen vorliegen werden, weil der Anwendungsbereich der personenbezogenen Meldungen entsprechend Art. 4 Nr. 1 DSGVO so ungemein weit ist. Wenn eine Meldung durch Zuordnung zu einer Kennnummer gespeichert wird, kann sie entsprechend Art. 4 Nr. 1 DSGVO („*Zuordnung (...) zu einer Kennnummer*“) mitunter schon nicht mehr als anonym gelten, weil die Hinweismeldung (anstelle eines Namens) einer eindeutigen Kennnummer zugeordnet werden kann, die für jede Hinweismeldung unterschiedlich ist.

2.8 Zu § 28 Abs. 3 HinSchG-E

§ 28 Abs. 3 Satz 2 HinSchG-E sieht vor, dass die Rechte der Personen, die Gegenstand einer Meldung sind oder die in der Meldung genannt werden, nicht beeinträchtigt werden dürfen.

In dem Zusammenhang stellt sich die Frage, ob die Abwesenheit von Beeinträchtigungen jeglicher Intensivität und von jeglichen in Gesetzen garantierten Rechten gemeint ist. Sofern die Bundesregierung nur auf die im HinSchG-E garantierten Rechte abstellen möchte und dabei nicht auch jegliche andere irgendwie gesetzlich garantierten Rechte gemeint sein sollen, so sollte dies deutlich gemacht werden.

Zudem ist fraglich, ob die Bundesregierung jegliche Beeinträchtigung von Rechten dafür ausreichen lässt oder ob durch die Formulierung vielmehr eine umfassende Interessenabwägung der sich gegenüberstehenden Rechte vorzunehmen ist. Zum Vergleich sei auf Art. 15 Abs. 4 Datenschutz-Grundverordnung verwiesen, in dem geregelt wird, dass „*Rechte und Freiheiten anderer Personen nicht (zu) beeinträchtigen*“ sind. In der Kommentarliteratur wird diese Passage so verstanden, dass nicht jegliche Formen von Beeinträchtigungen unzulässig sind, sondern eine umfassende Interessenabwägung zwischen den gegenüberstehenden Rechten vorzunehmen ist. Daher stellt sich die Frage, ob im Anwendungsbereich § 28 Abs. 3 Satz 2 HinSchG-E ebenfalls eine umfassende Interessenabwägung vorzunehmen ist.

2.9 Befugnis zur Regelung von Ausnahmen für Rechte und Pflichten aus DS-GVO

In Erwägungsgrund 84 S. 1 und S.2 der HinSch-RL teilt der unionale Gesetzgeber den Mitgliedstaaten mit, auf welcher Grundlage diese Beschränkungen von Betroffenenrechten und den für deren Erfüllung bestehende Pflichten im nationalen Recht vorsehen können. Dies sind Art. 23 Abs. 1 lit. e und i DSGVO. Auf Grundlage dieser Bestimmung kann der mitgliedstaatliche Gesetzgeber ausdrücklich Pflichtenausnahmen für DSGVO-Pflichten im nationalen Recht regeln.

Darüber hinaus wird auch deutlich erkennbar, dass der unionale Gesetzgeber nationalen Gesetzgebern einen ausdrücklichen Auftrag zur Regelung von Ausnahmen erteilt. Erwägungsgrund 84 Satz 3 der HinSch-RL lautet wie folgt:

*„Die Mitgliedstaaten sollten die Wirksamkeit dieser Richtlinie gewährleisten, indem sie unter anderem **erforderlichenfalls** die **Ausübung bestimmter Datenschutzrechte** betroffener Personen gemäß Artikel 23 Absatz 1 Buchstaben e und i und Artikel 23 Absatz 2 der Verordnung (EU) 2016/679 durch gesetzgeberische Maßnahmen **einschränken**, **soweit und solange** dies **notwendig** ist, um **Versuche, Meldungen zu behindern**, **Folgemaßnahmen** — insbesondere Untersuchungen — zu **verhindern**, zu **unterlaufen** oder zu **verschleppen** oder Versuche, die **Identität der Hinweisgeber festzustellen**, zu **verhüten und zu unterbinden**."*

An dieser Stelle wird der gesetzgeberische Auftrag an den nationalen Gesetzgeber deutlich. Es ist klar erkennbar, dass nationale Parlamente die aus der DSGVO heraus bestehenden Betroffenenrechte einschränken sollen, um die Wirksamkeit der zur Umsetzung der Richtlinie erlassenen Bestimmungen zu gewährleisten. Der HinSchG-E enthält genauso wie der Referentenentwurf allerdings bislang noch gar keine Einschränkungen, die sich unmittelbar auf Datenschutzrechte im Kontext von Whistleblowing und Pflichten von Unternehmen unter der DSGVO beziehen. In der Gesetzesbegründung wird darauf verwiesen, dass das BDSG schon die notwendigen Ausnahmetatbestände vorsieht. Es heißt hierzu wie folgt:

„Die notwendigen Ausnahmetatbestände haben indes bereits Eingang in das BDSG gefunden. Über die im Rahmen des § 29 Absatz 1 BDSG geforderte Interessenabwägung lässt sich der erforderliche Gleichlauf zwischen dem Vertraulichkeitsschutz und datenschutzrechtlichen Informationspflichten und Auskunftsrechten herstellen. Nach § 29 Absatz 1 Satz 1 BDSG treffen den datenschutzrechtlich Verantwortlichen keine Informationspflichten, soweit dies Informationen offenbaren würde, die ihrem Wesen nach geheim gehalten werden müssen. Nach § 29 Absatz 1 Satz 2 BDSG besteht das Recht zur Auskunft der betroffenen Person nicht, soweit durch die Auskunft Informationen offenbar würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach geheim gehalten werden müssen. Soweit Informationen dem Vertraulichkeitsgebot unterliegen, sind diese nach § 29 Absatz 1 BDSG grundsätzlich geheim zu halten."

Das BDSG kennt jedoch nur allgemeine Ausnahmetatbestände und keine solchen, die speziell für den Anwendungsbereich des HinSchG-E gelten sollen. Es hätte viele Vorteile für die Rechtssicherheit, wenn es spezielle Regelungen für Ausnahmen im Kontext von Whistleblowing oder zumindest Verweise (bspw. „§ X gilt entsprechend") gäbe. Insgesamt kennt der in der Gesetzesbegründung erwähnte § 29 BDSG auch nicht Ausnahmen für alle

relevanten Betroffenenrechte, sondern nur zu Art. 14 DSGVO, Art. 15 DSGVO und Art. 34 DSGVO. Für die ebenso praxisrelevanten Rechte aus Art. 13 DSGVO und Art. 16-21 DSGVO gibt es keinen Hinweis darauf, dass der Gesetzgeber Beschränkungen vorgesehen hat oder diese für erforderlich hält. Der unionale Gesetzgeber hat in dem Erwägungsgrund zur Richtline verdeutlicht, dass es im nationalen Recht speziell für das Thema „Whistleblowing" vorgesehen Ausnahmen bedarf.

- Zu den Informationspflichten und der fehlenden Ausnahme für Art. 13 DSGVO

  Es ist zu beachten, dass § 29 Abs. 1 BDSG nur für Datenverarbeitungen gilt, bei denen personenbezogene Daten nicht bei der betroffenen Person erhoben wurden. Somit gilt die Ausnahme aus § 29 Abs. 1 Satz 1 BDSG von vornherein nur für Art. 14 DSGVO aber nie für Art. 13 DSGVO. Es sind jedoch auch Konstellationen denkbar, in denen eine Anwendbarkeit von Art. 13 DSGVO problematisch ist. Gerade weil Art. 13 Abs. 4 DSGVO im Gegensatz zu Art. 14 Abs. 5 DSGVO nur eine sehr enge, sehr begrenzt anwendbare Ausnahme enthält, sollte der Gesetzgeber in Bezug auf Art. 13 DSGVO eine Ausnahme regeln. Dies wäre zumindest in der Gestalt denkbar, dass der § 29 Abs. 1 BDSG im Kontext von Whistleblowing auch für die Pflichten aus Art. 13 DSGVO gilt.

- Zu den Betroffenenrechten und den fehlenden Ausnahmen für Art. 16-21 DSGVO

  § 29 Abs. 1 BDSG ist mit Blick auf die Betroffenenrechte ausschließlich auf ein Betroffenenrecht (Art. 15 DSGVO) anwendbar. In der Gesetzesbegründung wird allerdings nur auf § 29 Abs. 1 BDSG verwiesen. Daher könnte man die Gesetzesbegründung so verstehen, dass in Bezug auf die Betroffenenrechte aus Art. 16-21 DSGVO gar keine Einschränkungen erforderlich wären. In der Praxis ist es jedoch so, dass auch für diese Betroffenenrechte Einschränkungen erforderlich sind.

  Mit Blick auf das Recht auf Berichtigung aus Art. 16 DSGVO kann es im Kontext des Whistleblowings dazu kommen, dass Hinweisgeber oder Beschuldigte oder anders Beteiligte eine Berichtigung von Daten verlangen. Wenn eine Berichtigung die Untersuchung oder andere Folgemaßnahmen beeinträchtigen würde, gäbe es trotzdem keine Ausnahme, die für diesen Fall greifen würde. Es ist auch denkbar, dass jemand von seinem Recht auf Löschung aus Art. 17 DSGVO oder von dem Recht auf Einschränkung der Verarbeitung aus Art. 18 DSGVO Gebrauch macht. Im Kontext von Whistleblowing sind viele Szenarien denkbar, in denen eine Löschung oder Einschränkung der Verarbeitung die ganze Untersuchung und damit auch alle Folgemaßnahmen gefährden könnten. Zudem gibt es die Mitteilungspflichten aus Art. 19 DSGVO, die mit den Rechten aus Art. 16-18 DSGVO zusammenhängen. Es ist auch denkbar, dass eine Mitteilung nach Art. 19 DSGVO dazu geeignet ist, die Untersuchung und andere Folgemaßnahmen komplett zu gefährden.

  Sofern im Kontext von Whistleblowing auch eine Einwilligung eingeholt wird, ist zudem Art. 20 DSGVO relevant. Es ist aber nicht ersichtlich, wieso betroffene Personen im Kontext von Whistleblowing ein Recht auf Datenübertragbarkeit aus Art. 20 DSGVO zustehen sollte. Das wäre weder im Sinne einer erfolgreich durchzuführenden Untersuchung, noch wäre es grundsätzlich für betroffene Personen sinnvoll, wenn die sich auf sie beziehenden Daten im Kontext von Whistleblowing auf Grundlage von Art. 20 DSGVO übertragen werden würden.

Von Unternehmen, die Hinweisgebersysteme betrieben, werden einige Datenverarbeitungen in der Praxis auch auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO vorgenommen. Wenn ein Unternehmen diese Rechtsgrundlage verwendet, steht den betroffenen Personen nach Art. 21 DSGVO ein Widerspruchsrecht zu. Es ist denkbar, dass auch eine auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO vorgenommene Datenverarbeitung für eine Untersuchung eines Vorfalls und Vornahme andere Folgemaßnahmen notwendig ist. In solchen Fällen sollte den betroffenen Personen jedoch kein Recht auf Widerspruch zustehen, soweit und solange dadurch die Untersuchung und andere Folgemaßnahmen beeinträchtigt werden könnten.

Der deutsche Gesetzgeber sollte daher bei den Ausnahmen nicht nur an Art. 14 DSGVO, Art. 15 DSGVO und Art. 34 DSGVO, sondern an alle Betroffenenrechte aus der DSGVO denken und entsprechende Ausnahmen im nationalen Recht regeln.

- Zeitliche Komponente des Regelungsauftrags und der Unanwendbarkeit von Pflichten aus der DSGVO

  Die erforderlichen Einschränkungen haben sowohl eine inhaltliche („*soweit*“) als auch eine zeitliche („*solange*“) Komponente. Der nationale Gesetzgeber ist durch den EU-Gesetzgeber ebenfalls dazu aufgefordert worden, die Dauer der Einschränkung von Rechten und Pflichten („*solange*“) zu regeln. Das BDSG kennt keine expliziten zeitweise erfolgenden Beschränkungen. Selbst wenn der Gesetzgeber also der Ansicht ist, dass das BDSG schon alle Ausnahmen enthält, sollte er in zeitlicher Hinsicht eine Regelung treffen. Es wäre bereits für die Rechtssicherheit positiv, wenn zumindest eine Regelung zur zeitlichen Komponente der Geltung der Ausnahmen getroffen werden würde.

2.10 Datenschutz-Folgenabschätzung

In der Orientierungshilfe der DSK zu Whistleblowing-Hotlines gehen die staatlichen Datenschutzaufsichtsbehörden davon aus, dass die Durchführung einer Datenschutz-Folgenabschätzung erforderlich ist (vgl. Ziffer E10 der Orientierungshilfe).

Wir regen daher erneut dringend an, dass die Datenschutz-Folgenabschätzung bereits im Gesetzgebungsverfahren durchgeführt wird. Gemäß Art. 35 Abs. 10 DS-GVO ist es möglich, dass eine Datenschutz-Folgenabschätzung bereits im Rahmen des Gesetzgebungsverfahrens erfolgt. Dann müssen die Verantwortlichen selbst keine Datenschutz-Folgenabschätzung nach Art. 35 Abs. 1 – 7 DS-GVO durchführen. Diese Möglichkeit wurde in Deutschland beispielsweise bereits beim „Patienten-Datenschutzgesetz“ genutzt, vgl. § 307 Abs. 1 Satz 3 SGB V. Ein vergleichbares Vorgehen in diesem Fall würde sämtliche öffentlichen und nicht-öffentlichen Einrichtungen, die Hinweisgebersysteme einsetzen, wesentlich von Bürokratieaufgaben entlasten, ohne dass dadurch ein Risiko für die Rechte und die Freiheiten der betroffenen Personen entstünde. Der Erfüllungsaufwand für die Wirtschaft wird nach dem Referentenentwurf bereits mit jährlich 200,9 Millionen Euro geschätzt. Es sollte vermieden werden, dass der Erfüllungsaufwand noch weiter ansteigt. Die Datenschutz-Folgenabschätzung im Gesetzgebungsverfahren durchzuführen, würde einem weiteren Anstieg des Erfüllungsaufwands entgegengenwirken.

Bitkom vertritt mehr als 2.700 Unternehmen der digitalen Wirtschaft, davon gut 2.000 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.