Bundesanzeiger
Herausgegeben vom
Bundesministerium der Justiz
www.bundesanzeiger.de

Bekanntmachung
Veröffentlicht am Mittwoch, 4. Mai 2022
BAnz AT 04.05.2022 B2

Bundesministerium des Innern und für Heimat

Bekanntmachung der Begründung zur IT-Sicherheitsverordnung Portalverbund – ITSiV-PV

Vom 14. April 2022

Nachstehend wird die Begründung zur IT-Sicherheitsverordnung Portalverbund vom 6. Januar 2022 (BGBl. I S. 18) bekannt gegeben (Anlage).

Berlin, den 14. April 2022

Bundesministerium
des Innern und für Heimat

Im Auftrag
Dr. Markus Richter

Anlage

Begründung
zur
IT-Sicherheitsverordnung Portalverbund – ITSiV-PV

A. Allgemeiner Teil

I. Zielsetzung und Notwendigkeit der Regelungen

Diese Verordnung definiert verbindlich die für die im Portalverbund und für die zur Anbindung an den Portalverbund genutzten IT-Komponenten notwendigen Standards zur Gewährleistung der IT-Sicherheit. Der Gewährleistung der IT-Sicherheit dienen auch solche Maßnahmen und Standards, die nicht rein produktbezogen sind, sondern die Einbettung der IT-Komponenten in das informationstechnische System beziehungsweise Verfahren betreffen. Die Verordnung ist notwendig und erforderlich zur Festlegung eines einheitlichen Schutzniveaus zur Vermeidung von Sicherheitslücken und Sicherheitsvorfällen. Ein unzureichendes Sicherheitsniveau oder gar Sicherheitslücken in einer der verwendeten IT-Komponenten können über den vernetzten Portalverbund die Sicherheit aller beteiligten Verwaltungseinrichtungen, der genutzten Verwaltungsnetze und der in den jeweiligen Verfahren bearbeiteten Daten mindestens beeinträchtigen (vgl. BT-Drucksache 18/11135, S. 93). Aufgrund der gewollten Vernetzung im Portalverbund besteht darüber hinaus zudem das Risiko, dass Angriffe oder Bedrohungen die Handlungsfähigkeit der Verwaltung insgesamt gefährden. Daher ist die Festlegung verbindlicher Vorgaben zur Gewährleistung eines einheitlichen und angemessenen IT-Sicherheitsniveaus durch diese Verordnung zwingend erforderlich (vgl. BT-Drucksache 18/11135, S. 93).

II. Wesentlicher Inhalt des Entwurfs

Die Verordnung basiert auf Erfahrungen mit der Umsetzung von IT-Sicherheitsvorgaben in der Bundesverwaltung und in den Ländern.

Wesentlicher Inhalt des Entwurfs ist (Portalverbund und unmittelbar angebundene IT-Komponenten):

- Die relevanten IT-Komponenten sind nach dem Stand der Technik abzusichern, wobei der Stand der Technik durch die Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) vorgegeben wird. Die Fortschreibung dieser Standards erfolgt durch das BSI im Benehmen mit den Ländern.
- Die IT-Komponenten sind auf der Grundlage eines IT-Sicherheitskonzeptes nach BSI IT-Grundschutz bzw. ISO/IEC 27001 abzusichern. Dabei ist mindestens die Standard-Absicherung nach BSI-Standard 200-2 umzusetzen.
- Die IT-Komponenten müssen Bestandteil eines Informationssicherheitsmanagements sein, das die Vorgaben des IT-Planungsrates hierzu umsetzt. Zudem müssen die IT-Komponenten Bestandteil eines IT-Notfallmanagements sein, das die Vorgaben der Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung des IT-Planungsrates erfüllt.
- Bestimmte IT-Komponenten, die einem erhöhten Sicherheitsrisiko ausgesetzt sind, müssen vor der Anbindung an den Portalverbund einem Webcheck und einem Penetrationstest unterzogen werden.

III. Alternativen

Keine

IV. Regelungskompetenz

Die Regelungskompetenz des Bundesministeriums des Innern und für Heimat folgt aus Artikel 91c Absatz 5 Grundgesetz (GG) in Verbindung mit § 5 Satz 1 des Onlinezugangsgesetzes (OZG).

V. Vereinbarkeit mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen

Die Verordnung ist mit dem Recht der Europäischen Union und mit völkerrechtlichen Verträgen, die die Bundesrepublik Deutschland abgeschlossen hat, vereinbar. Ein Notifizierungsverfahren nach Richtlinie 2015/1535/EU wurde geprüft. Die Durchführung eines solchen Notifizierungsverfahrens ist entbehrlich, da die referenzierten Standards technikneutral sind und dadurch keine Hemmnisse für den freien Daten- und Warenverkehr in der Europäischen Union zu erkennen sind.

VI. Regelungsfolgen

Die Verordnung konkretisiert im Wesentlichen die im Rahmen des Aufbaus und der Inbetriebnahme des Portalverbundes bereits bestehenden Verpflichtungen zur Gewährleistung der IT-Sicherheit.

Ein Mehraufwand für Bund und Länder ist hinsichtlich der Erstellung und Aktualisierung von IT-Sicherheitskonzepten und hinsichtlich der Kosten für entsprechende Penetrationstests und Webchecks und für die Weiterentwicklung von Technischen Richtlinien zu erwarten. Die direkten Prüfkosten (Planung und Durchführung der Prüfungen, Erstellung der Prüfberichte und gegebenenfalls notwendige Abstimmungen mit der jeweils verantwortlichen Stelle) hängen wesentlich von der Größe und dem Komplexitätsgrad des entsprechenden Informationsverbundes und von den eingesetzten IT-Komponenten ab. Daher ist eine Quantifizierung des Mehraufwandes an dieser Stelle nicht möglich.

Eine finanzielle oder zeitliche Mehrbelastung für Bürgerinnen und Bürger sowie für die Wirtschaft ist nicht zu erwarten. Auswirkungen auf Einzelpreise oder das Preisniveau sind ebenfalls nicht zu erwarten. Weitere unmittelbare oder mittelbare Regelungsfolgen sind nicht ersichtlich.

1. Rechts- und Verwaltungsvereinfachung

   keine

2. Nachhaltigkeitsaspekte

   Nachhaltigkeitsaspekte sind nicht betroffen.

3. Haushaltsausgaben ohne Erfüllungsaufwand

   keine

4. Erfüllungsaufwand

   Für die Bürgerinnen und Bürger und für die Wirtschaft entsteht kein Erfüllungsaufwand.

   Für die Verwaltung ändert sich der jährliche Erfüllungsaufwand um rund 19 137 Tsd. Euro. Davon entfallen 1 133 Tsd. Euro an jährlichem Erfüllungsaufwand auf den Bund und 18 004 Tsd. Euro auf die Länder, einschließlich Kommunen (vor allem für Aktualisierung der Sicherheitskonzepte, Durchführung von Penetrationstests und Webchecks). Der einmalige Erfüllungsaufwand beträgt rund 102 407 Tsd. Euro. Davon entfallen 2 518 Tsd. Euro an einmaligem Erfüllungsaufwand auf den Bund und 99 889 Tsd. Euro auf die Länder (inkl. Kommunen). Der größte einmalige Aufwand in Höhe von 88 734 Tsd. Euro entsteht, ausgehend von 11 000 Kommunen, hierbei im Zuge der Erstellung und Aktualisierung von Sicherheitskonzepten gemäß Basis-Absicherung nach IT-Grundschutz (vgl. § 1 Absatz 4 Nummer 2). Für die Aktualisierung der Sicherheitskonzepte gemäß Basis-Absicherung entsteht in den Ländern ein jährlicher Erfüllungsaufwand von 8 874 Tsd. Euro.

   Der Erfüllungsaufwand ist somit im Wesentlichen auf die Entwicklung Technischer Richtlinien (TR) durch das BSI, das Erstellen und Aktualisieren von IT-Sicherheitskonzepten (einschließlich Erstellung der Eigenerklärung), die Durchführung von Webchecks und Penetrationstests und die Begleitung der Webchecks und Penetrationstests durch den Bund und die Länder zurückzuführen.

5. Weitere Kosten

   keine

6. Weitere Regelungsfolgen

   Keine

VII. Befristung; Evaluierung

Eine Befristung ist nicht angezeigt. Veranlasst durch den schnellen technischen Fortschritt in der Informationstechnik erfolgt ein fortlaufendes Monitoring der Verordnung und der durch sie gesetzten Standards durch das Bundesministerium des Innern und für Heimat, soweit die Verordnung nicht bereits dynamische Verweise auf Standards enthält. Damit wird sichergestellt, dass die Verordnung regelmäßig an den Fortschritt der Informationstechnik und die damit einhergehenden geänderten IT-Sicherheitsanforderungen angepasst wird.

Eine Evaluierung findet statt.

Ziel der Regelungen ist es, die in den IT-Systemen des Portalverbundes verarbeiteten Daten der Bürgerinnen und Bürger und der Organisationen vor Manipulation, Verlust und unbefugter Offenbarung zu schützen. Dies soll durch Implementierung und Aufrechterhaltung eines angemessenen IT-Sicherheitsniveaus im gesamten Portalverbund und bei den für die Anbindung an den Portalverbund genutzten IT-Komponenten erreicht werden. Die Evaluierung wird auf der Grundlage eines standardisierten Fragebogens in Bund und Ländern stattfinden, der u. a. auch den für die Umsetzung der Sicherheitsanforderungen notwendigen Ressourcenbedarf betrachtet.

Die Evaluierung findet drei Jahre nach Inkrafttreten der Rechtsverordnung statt. Die genauen Kriterien für die Evaluierung des standardisierten Fragebogens (z. B. Anzahl und Art der Sicherheitsvorfälle) werden zu diesem Zeitpunkt zwischen Bund und Ländern abgestimmt. Die genauen Kriterien sind auf der Grundlage des erwarteten Nutzens der Rechtsverordnung (sicherer Betrieb der IT-Komponenten des Portalverbundes und der IT-Komponenten zur Anbindung an den Portalverbund) festzulegen.

Im Rahmen der Evaluierung soll auch überprüft werden, ob künftig vor Inkraftsetzung neuer oder geänderter Technischer Richtlinien in Zusammenarbeit mit ausgewählten betroffenen Stellen in Bund und/oder Ländern und/oder Kommunen die Durchführung eines „Proof-of-Concept“ (PoC) empfehlenswert ist.

B. Besonderer Teil

Zu § 1 (Begriffsbestimmungen)

Die Absätze 1 und 2 verweisen hinsichtlich der in der Verordnung verwendeten Begriffe auf § 2 OZG sowie § 2 BSI-Gesetz. Die Verweisungen bieten sich an, da in den genannten Vorschriften grundlegende Begriffe der OZG-Infrastruktur und der IT-Sicherheit bereits vordefiniert sind.

Absatz 3 legt den Anwendungsbereich der Verordnung fest. Der dort bezeichnete „Portalverbund“ ist nach § 2 Absatz 1 OZG eine technische Verknüpfung der Verwaltungsportale von Bund und Ländern, über die der Zugang zu Verwaltungsleistungen auf unterschiedlichen Portalen angeboten wird. IT-Komponenten im Portalverbund sind IT-Anwendungen, Basisdienste und Schnittstellen, die für den Betrieb des Verbundes und für die Abwicklung der Verwaltungsleistungen im Portalverbund erforderlich sind. Dazu zählen u. a. das Online Gateway des Portalverbunds,

die interoperablen Nutzerkonten von Bund und Ländern mit elektronischen Postfächern, das Datenschutzcockpit, der Datensafe, der elektronische Bezahldienst und die Suchfunktion.

Durch die Vernetzung der IT-Komponenten der zahlreichen Verbundteilnehmer entsteht ein Verbundrisiko für die Verfügbarkeit, die Integrität und die Vertraulichkeit der darin verarbeiteten Daten. Ein unzureichendes Sicherheitsniveau in einer der vernetzten IT-Komponenten kann die Sicherheit aller angeschlossenen Verwaltungseinrichtungen und damit die Handlungsfähigkeit der Verwaltung insgesamt gefährden. Der vernetzte Verbund ist daher gemäß Absatz 3 angemessen abzusichern.

Zur Gewährleistung einer lückenlosen und wirksamen Absicherung sieht die Ermächtigungsgrundlage des § 5 Satz 1 OZG vor, dass auch die zur Anbindung an den Portalverbund genutzten IT-Komponenten mit angemessenen Sicherheitsstandards versehen werden. Absatz 4 setzt dies durch ein abgestuftes System um:

Unmittelbar an den Portalverbund angeschlossene IT-Komponenten im Sinne des Absatzes 4 Nummer 1 sind diejenigen Komponenten, die über technische Schnittstellen Daten unmittelbar mit dem Portalverbund austauschen. Dazu zählen z. B. die von öffentlichen Stellen (unmittelbare und mittelbare Bundes- und Landesverwaltung einschließlich der Kommunen) betriebenen Fach- und Themenportale sowie EfA-Online-Dienste, die an die Nutzerkonten von Bund und Ländern angeschlossen sind. Nicht dazu zählen Portale, die keine eigene Schnittstelle zum Portalverbund besitzen und lediglich auf weiterführende Informationen innerhalb des Verbunds verlinken (Informationsportale).

Eine unmittelbare Anbindung an den Portalverbund bedingt, dass über die weitreichenden Zugriffsmöglichkeiten der Schnittstellen erhöhte Sicherheitsrisiken für den Portalverbund entstehen können (Gefährdung der Vertraulichkeit, der Integrität und der Verfügbarkeit). In diesem Fall ist eine angemessene Steuerung der Risiken nur möglich, wenn die in § 2 genannten Maßnahmen umgesetzt werden.

Eine mittelbare Anbindung an den Portalverbund nach § 1 Absatz 4 Nummer 2 liegt vor, wenn öffentliche Stellen (z. B. Kommunen) Komponenten nach § 1 Absatz 4 Nummer 1 nicht eigenverantwortlich betreiben, sondern lediglich mitnutzen und hierzu ihre IT-Systeme an sie anschließen. Beispiel: eine Kommune stellt ihre digitalen Verwaltungsleistungen in ein übergeordnetes, von einer anderen Stelle betriebenes Portal ein oder nutzt einen von einer anderen Stelle betriebenen EfA-Online-Dienst.

Mit der lediglich mittelbaren Anbindung nach § 1 Absatz 4 Nummer 2 geht ein geringeres Gefährdungspotential (Gefährdung der Vertraulichkeit, der Integrität und der Verfügbarkeit) für den Portalverbund einher. Die in § 3 genannten Maßnahmen bilden dieses geringere Gefährdungspotential ab.

Zu § 2 (Portalverbund und unmittelbar angebundene IT-Komponenten)

Absatz 1: Absatz 1 fordert für bestimmte IT-Komponenten die Umsetzung von Maßnahmen nach dem Stand der Technik.

Absatz 2: Absatz 2 enthält eine Vermutungsregel dahingehend, dass der Stand der Technik im Sinne des Absatz 2 dann eingehalten ist, wenn die in der Anlage zu dieser Verordnung aufgeführten Standards in Form von Technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik in der jeweils geltenden Fassung umgesetzt werden. Der verantwortlichen Stelle ist es unbenommen, den Stand der Technik auf andere Weise herbeizuführen. Sie trägt hierfür jedoch die Nachweispflicht, dass die alternativ gewählten Maßnahmen den Stand der Technik ebenso gut gewährleisten wie die in der Anlage aufgeführten Technischen Richtlinien. Nach Satz 2 werden die in der Anlage genannten Technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik zur Transparenzsicherung im Bundesanzeiger durch Verweis auf die Internetseite des Bundesamtes für Sicherheit in der Informationstechnik bekanntgegeben:

https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Moderner-Staat/Online-Zugangsgesetz/IT-Sicherheitsverordnung_PVV/IT-Sicherheitsverordnung_ITSiV-PVV.html

Satz 3 der Regelung gewährt den Verantwortlichen des IT-Betriebes eine Übergangszeit zur Umstellung der eigenen Sicherheitsmaßnahmen und zur Anpassung auf die Fortschreibungen.

Absatz 3: Die Erarbeitung weiterer oder Fortschreibung bestehender Technischer Richtlinien durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) erfolgt im Rahmen einer intensiven Konsultation des BSI mit den Ländern, da die praktischen Erfahrungen bei der Umsetzung der Vorgaben dieser Verordnung und die Gewährleistung der entsprechend hierauf bezogenen IT-Sicherheit in die Fortschreibung der verbindlichen Standards nach dieser Verordnung einfließen sollen.

Die Letztentscheidung über die Anerkennung erarbeiteter beziehungsweise fortgeschriebener Technischer Richtlinien liegt bei dem Bundesministerium des Innern und für Heimat. Dies folgt aus der Kompetenzzuschreibung des § 5 Satz 1 OZG.

Absatz 4: Nach Absatz 4 müssen die genutzten IT-Komponenten Bestandteil eines Informationssicherheitsmanagementsystems sein, welches die Vorgaben der aktuell gültigen Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung des IT-Planungsrates umsetzt:

https://www.it-planungsrat.de/fileadmin/beschluesse/2019/Beschluss2019-04_TOP12_Anlage_Leitlinie.pdf

Insofern handelt es sich hierbei um bereits bestehende Anforderungen zur Gewährleistung einer angemessenen IT-Sicherheit.

Das Informationssicherheitsmanagementsystem ist während der gesamten Betriebsdauer der IT-Komponenten ununterbrochen aufrechtzuerhalten. Letztgenanntes ist notwendig, um durchweg ein angemessenes IT-Sicherheitsniveau zu gewährleisten.

Absatz 5: Absatz 5 normiert ausdrücklich die Erstellung und Umsetzung eines IT-Sicherheitskonzeptes nach BSI IT-Grundschutz oder nach ISO/IEC 27001, wobei als Mindestanforderung die Umsetzung der Standardabsicherung nach den BSI-Standards 200-1, 200-2, 200-3 vorgesehen ist. Als Hilfsmittel kann die Zuordnungstabelle der Maßnahmen nach ISO/IEC 27001 zum IT-Grundschutz verwendet werden:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/Zuordnung_ISO_und_IT_Grundschutz.html

Verantwortliche Stellen der Bundesverwaltung müssen ein Sicherheitskonzept nach den BSI-Standards 200-1, 200-2, 200-3 erstellen und umsetzen (Standard-Absicherung).

Im Rahmen dieses IT-Sicherheitskonzeptes gilt der Grundsatz, dass Nutzer eines Organisationskontos sich für die im Portalverbund verfügbaren elektronischen Verwaltungsleistungen von Bund und Ländern einheitlich über ein nach § 87a Absatz 6 der Abgabenordnung in der Steuerverwaltung eingesetztes sicheres Verfahren identifizieren und authentisieren können. Die verantwortliche Stelle kann nach eigenem Ermessen externe Dienstleister mit der Erstellung des IT-Sicherheitskonzeptes beauftragen. Bei Einbindung externer Dienstleister (z. B. RZ-Dienstleister) ist die verantwortliche Stelle (z. B. Behörde) weiterhin verantwortlich für die Einhaltung der Vorgaben dieser Verordnung. Die im föderalen Digitalisierungsprogramm bereitgestellten Konjunkturpaketmittel beinhalten standardmäßig auch finanzielle Mittel für die Erstellung eines IT-Sicherheitskonzeptes.

Absatz 6: Absatz 6 legt fest, dass für bestimmte IT-Komponenten vor Anbindung an den Portalverbund Penetrationstests und Webchecks durchzuführen sind, da ein angemessener Schutz dieser Komponenten von herausragender Bedeutung für den sicheren und regelkonformen Betrieb des Portalverbundes ist. Jede verantwortliche Stelle bestimmt auf der Grundlage der Schutzbedarfskategorien nach BSI IT-Grundschutz die relevanten IT-Komponenten in ihrem jeweiligen Zuständigkeitsbereich. Nutzerkonto, elektronischer Bezahldienst, Postfach und Datensafe zählen auf jeden Fall zu diesen IT-Komponenten.

Absatz 7: Nach größeren Änderungen, spätestens jedoch nach 3 Jahren, sind Penetrationstests und Webchecks zu wiederholen, um gegebenenfalls durch technische Änderungen neu entstandene Sicherheitslücken zu identifizieren und durch angemessene Sicherheitsmaßnahmen zu schließen.

Absatz 8: Penetrationstests und Webchecks sollen vorzugsweise durch das Bundesamt für Sicherheit in der Informationstechnik (BSI), durch Fachbehörden für Informationssicherheit der Länder (z. B. Landesämter für Sicherheit in der Informationstechnik, Cybersicherheitsagenturen, CERT) oder durch vom Bundesamt für Sicherheit in der Informationstechnik zertifizierte IT-Sicherheitsdienstleister durchgeführt werden.

Absatz 9: Stehen die Ressourcen nach Absatz 8 nicht oder in nicht ausreichendem Umfang zur Verfügung, um die Anforderungen des § 2 Absatz 6 umzusetzen, können ersatzweise auch IT-Sicherheitsdienstleister ohne Zertifizierung mit den Prüfungen beauftragt werden, sofern sie für die Durchführung von Penetrationstests nachweislich die entsprechende Fachkunde nach „Personenzertifizierung: Programm IS-Penetrationstester“ (Kapitel 2.1.1 und 2.1.3) des Bundesamtes für Sicherheit in der Informationstechnik in der jeweils geltenden Fassung besitzen:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/IS-Penetrationstester.pdf

Penetrationstester sollen eine für die Durchführung des entsprechenden Penetrationstests angemessene fachspezifische Berufserfahrung auf dem Gebiet von technischen Sicherheitsanalysen und Penetrationstests besitzen. Zudem müssen die Prüfungen nach den Vorgaben des BSI in der jeweils geltenden Fassung durchgeführt werden:

1. Praxis-Leitfaden für IS-Penetrationstests

   https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Leitfaden_Penetrationstest.pdf

2. Praxis-Leitfaden für den IS-Webcheck

   https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Leitfaden_Webcheck.pdf

Bei Webchecks und Penetrationstests ist die Unabhängigkeit der Prüfung durch die beauftragende Institution sicherzustellen:

1. IT-Dienstleister, die im Auftrag den IT-Betrieb sicherstellen, dürfen nicht mit Penetrationstests und Webchecks beauftragt werden, da dabei gegebenenfalls Interessenkonflikte entstehen könnten. Die Möglichkeit allein reicht aus, um die Unabhängigkeit der Prüfung zu gefährden.
2. IT-Prüfer, die in den letzten 3 Jahren vor Durchführung der Prüfung (Penetrationstest oder Webcheck) im Bereich des Prüfgegenstandes bei der geprüften Institution beratend tätig waren, dürfen nicht mit Prüfungen beauftragt werden.

Absatz 10: Die Ergebnisse der Penetrationstests und Webchecks sind in einem Prüfbericht zu dokumentieren und bei den jeweils in Bund und Ländern verantwortlichen Stellen zu hinterlegen. Bund und Länder legen hierfür das jeweils in ihrem Bereich notwendige Formerfordernis fest. Gefundene Mängel sind zu beseitigen und die Beseitigung ist zu dokumentieren.

Absatz 11: Die genutzten IT-Komponenten müssen Bestandteil eines IT-Notfallmanagements sein, das die Vorgaben der Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung des IT-Planungsrates erfüllt. Das IT-Notfallmanagement ist während der gesamten Betriebsdauer der IT-Komponenten ununterbrochen aufrechtzuerhalten. Dadurch ist die Verfügbarkeit der im Portalverbund verarbeiteten Daten auch im Notfall sichergestellt.

Zum Zeitpunkt des Inkrafttretens ist der aktuelle Stand nach Beschluss des IT-Planungsrat 4/2019 abrufbar unter:

https://www.it-planungsrat.de/fileadmin/beschluesse/2019/Beschluss2019-04_TOP12_Anlage_Leitlinie.pdf

Absatz 12: Nach Absatz 12 ist die jeweils verantwortliche Stelle zuständig für die Umsetzung der Vorgaben nach dieser Verordnung. Verantwortliche Stelle meint die für den Betrieb verantwortliche Institution. Die Regelung macht deutlich, dass die Einbindung von Dienstleistern nicht von der Pflicht zur Einhaltung der Verordnung entbindet. Die Einhaltung dieser Vorgaben durch beauftragte Dienstleister ist daher vertraglich sicherzustellen. Die Umsetzung der Vorgaben dieser Verordnung ist für IT-Komponenten des Portalverbundes durch eine jährliche Eigenerklärung der verantwortlichen Stelle zu dokumentieren. Das Bundesministerium des Innern und für Heimat stellt ein einheitliches Muster für die Eigenerklärung zur Verfügung:

https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Moderner-Staat/Online-Zugangsgesetz/IT-Sicherheitsverordnung_PVV/IT-Sicherheitsverordnung_ITSiV-PVV.html

Absatz 13: Bund und Länder bestimmen jeweils sowohl die zentralen Stellen, bei denen die entsprechenden Eigenerklärungen zu hinterlegen sind, als auch das genaue Verfahren zur Abgabe der Erklärungen. Sie legen das jeweils in ihrem Bereich notwendige Formerfordernis fest. Dies soll sicherstellen, dass jeweils bereits vorhandene bundes- und landesspezifische Rahmenbedingungen Berücksichtigung finden. Für den Bund ist das Bundesamt für Sicherheit in der Informationstechnik die zentrale Stelle.

Zu § 3 (Mittelbar angebundene IT-Komponenten)

Da die Stellen nach § 1 Absatz 4 Nummer 2 keine unmittelbare Schnittstelle zum Portalverbund aufweisen, wird von ihnen lediglich die Erstellung und Umsetzung eines IT-Sicherheitskonzeptes gefordert. Kommunen können das IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung in der jeweils geltenden Fassung nutzen:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Basis_Absicherung_Kommunalverwaltung.html

Alternativ kann der Erstellung des Sicherheitskonzeptes auch ein vom jeweiligen Land anerkannter Standard zugrunde gelegt werden, der der Basis-Absicherung des BSI-Standards 200-2 entspricht.

Stellen nach § 1 Absatz 4 Nummer 2 müssen zusätzlich auch die von ihrem Diensteanbieter festgelegten Nutzungsbedingungen erfüllen. Nutzungsbedingungen legen der jeweils konkreten Risikosituation angemessene IT-Sicherheitsmaßnahmen für die mittelbare Anbindung an den Portalverbund schriftlich fest. Dies kann in Form eines eigenständigen Vertrages, eines Security Service Level Agreements, einer sonstigen Anlage o. Ä. zu einem bereits bestehenden Vertrag erfolgen.

Zu § 4 (Übergangsregelung)

Die in § 4 niedergelegte Übergangsregelung dient dazu, den Verantwortlichen von bereits im Betrieb befindlichen oder kurzfristig in Betrieb zu setzenden IT-Komponenten die Möglichkeit zu eröffnen, diese planmäßig zu betreiben.

Eine unmittelbare, zeitlich nicht aufgeschobene Verpflichtung aus dieser Verordnung könnte dazu führen, dass entsprechende IT-Komponenten bis zur Erfüllung der Anforderungen nicht mehr betrieben oder nicht in Betrieb genommen werden dürfen. Dies wäre unverhältnismäßig.