Bundesamt
für Sicherheit in der
Informationstechnik

CON.2 Datenschutz

1. Beschreibung

1.1. Einleitung

Im Gegensatz zur Informationssicherheit, die primär dem Schutz der datenverarbeitenden Institution dient, ist es Aufgabe des Datenschutzes, natürliche Personen davor zu schützen, dass Institutionen oder Stellen mit ihren Verarbeitungstätigkeiten zu intensiv in die Grundrechte und Grundfreiheiten der Personen eingreifen. Das Grundgesetz für die Bundesrepublik Deutschland gewährleistet das Recht von Bürgerinnen und Bürgern, grundsätzlich selbst über die Verwendung ihrer personenbezogenen Daten zu bestimmen. Die Datenschutzgesetze des Bundes und der Bundesländer nehmen darauf Bezug, wenn sie den Schutz des Rechts auf informationelle Selbstbestimmung hervorheben. Die EU-Grundrechtecharta formuliert in Artikel 8 unmittelbar das Recht auf den Schutz personenbezogener Daten (Absatz 1), hebt die Notwendigkeit einer Rechtsgrundlage zur Datenverarbeitung hervor (Absatz 2) und schreibt die Überwachung der Einhaltung von Datenschutzvorschriften durch eine unabhängige Stelle vor (Absatz 3). Die Datenschutz-Grundverordnung (DSGVO) führt diese Anforderungen der Grundrechtecharta näher aus. Von zentraler Bedeutung ist dabei der Artikel 5 DSGVO, der die Grundsätze für die Verarbeitung personenbezogener Daten auflistet, die teilweise auch als Schutzziele verstanden werden können. Neben der DSGVO sind das Bundesdatenschutzgesetz (BDSG) und die Datenschutzgesetze der Bundesländer sowie weitere bereichsspezifische Regelungen wie beispielsweise das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) zu berücksichtigen.

Zugespitzt sind im Rahmen des operativen Datenschutzes vier Typen von Risiken, die mit unterschiedlichen Ausprägungen von Schutzmaßnahmen zu verringern sind, zu unterscheiden:

- Risikotyp A: Der Grundrechtseingriff bei natürlichen Personen durch die Verarbeitung ist nicht hinreichend milde gestaltet.
- Risikotyp B: Die Maßnahmen zur Verringerung der Eingriffsintensität einer Verarbeitung sind, in Bezug auf die Gewährleistungsziele, nicht vollständig oder werden nicht hinreichend wirksam betrieben oder nicht in einem ausreichenden Maße stetig kontrolliert, geprüft und beurteilt.
- Risikotyp C: Die Maßnahmen, die nach der Informationssicherheit geboten sind (vgl. z. B. IT-Grundschutz nach BSI), sind nicht vollständig oder werden nicht hinreichend wirksam betrieben oder werden nicht in einem ausreichenden Maße stetig kontrolliert, geprüft und beurteilt.
- Risikotyp D: Die Maßnahme der Informationssicherheit werden nicht ausreichend datenschutzgerecht, im Sinne des Risikotyp A und Risikotyp B, betrieben.

Die Prüfung der Verhältnismäßigkeit des Grundrechtseingriffs einer Verarbeitung ist nicht vom SDM umfasst. Diese rechtliche Prüfung sowie die Prüfung der Rechtsgrundlage (vergleiche insbesondere Art. 6 und 9 DS-GVO) und des Verarbeitungszwecks müssen vor der Anwendung des SDM erfolgen. Somit ist die Behandlung des zuvor genannten Risikotyps A nicht unmittelbar Gegenstand der Anwendung des SDM. Wird ein oder werden mehrere Risikotypen nicht betrachtet oder nicht hinreichend zwischen den Risiko-Typen differenziert, dann besteht die Gefahr, dass das informationelle Selbstbestimmungsrecht der betroffenen Person nicht gesetzeskonform gewährleistet werden kann.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (kurz: Datenschutzkonferenz, DSK) hat mit dem Standard-Datenschutzmodell (SDM) eine Methode entwickelt, welche die in den deutschen und europäischen Rechtsvorschriften genannten technischen und organisatorischen Maßnahmen auf der Basis von sieben Schutz- beziehungsweise Gewährleistungszielen systematisiert. Damit dient das Modell den für die Datenverarbeitung verantwortlichen und als Auftragsverarbeiter beteiligten Stellen, erforderliche Maßnahmen systematisch zu planen sowie umzusetzen. Es fördert somit die datenschutzgerechte Ausgestaltung und Organisation von informationstechnischen Verfahren, Anwendungen und Infrastrukturen. Andererseits bietet das Modell den Datenschutzaufsichtsbehörden eine Möglichkeit, mit einer einheitlichen Systematik zu einem transparenten, nachvollziehbaren und belastbaren Gesamturteil über eine Verarbeitung zu gelangen. Das SDM ist als Methode geeignet, die Wirksamkeit der technischen und organisatorischen Maßnahmen einer Datenverarbeitung auf der Grundlage und nach den Kriterien der DSGVO regelmäßig zu überprüfen und fachgerecht zu bewerten.

Das SDM nimmt bei der Auswahl geeigneter technischer und organisatorischer Maßnahmen die Perspektive der Betroffenen und deren Grundrechtsausübung ein und unterscheidet sich daher grundlegend von der Sicht des IT-Grundschutzes. Dieser legt den Schwerpunkt vorrangig auf die Informationssicherheit und soll die datenverarbeitenden Institutionen schützen. Für die Risikobeurteilung und die anschließende Auswahl von Maßnahmen nach dem SDM ist hingegen die Beeinträchtigung maßgeblich, die Betroffene durch die Datenverarbeitung der Institution hinnehmen müssen.

Vor diesem Hintergrund ist zwischen der Auswahl von Maßnahmen zur Gewährleistung der Informationssicherheit für Institutionen und der Auswahl von Maßnahmen zur Gewährleistung des Datenschutzes zu unterscheiden: Die IT-Grundschutz-Methodik dient vorrangig der Informationssicherheit, das Standard-Datenschutzmodell dient der Umsetzung der datenschutzrechtlichen Anforderungen (insbesondere der Grundsätze aus Artikel 5 DSGVO und der Betroffenenrechte aus Kapitel III DSGVO). Das SDM hat daher die folgenden Ansprüche:

- Es überführt datenschutzrechtliche Anforderungen in einen Katalog von Gewährleistungszielen.
- Es gliedert die betrachteten Verfahren in die Komponenten Daten, Systeme und Dienste (inkl. Schnittstellen) sowie Prozesse.
- Es berücksichtigt die Einordnung von Verarbeitungstätigkeiten basierend auf den Risikostufen "kein oder gering", "normal" und "hoch" gemäß DSGVO in die Schutzbedarfsstufen „normal“ und „hoch“, insbesondere mit Auswirkungen auf der Ebene der Sachbearbeitung mit ihren Fachverfahren, die von Anwendungen und IT-Infrastruktur unterstützt werden.
- Es bietet einen Katalog mit standardisierten Schutzmaßnahmen.

Der Referenzmaßnahmen-Katalog des SDM umfasst Maßnahmen, die auf Informationsverbünde oder Verfahren (Verarbeitungen) sowie auf die gesamte Institution im Rahmen eines Datenschutzmanagementprozesses anzuwenden sind.

Die Prüfung der Verhältnismäßigkeit des Grundrechtseingriffs einer Verarbeitung ist nicht vom SDM umfasst. Diese rechtliche Prüfung sowie die Prüfung der Rechtsgrundlage nach Artikel 6 und gegebenenfalls des Artikels 9 DSGVO müssen erfolgen, bevor das SDM angewendet wird. Somit wird der Risikotyp A nicht im Rahmen des SDM selbst behandelt.

1.2. Zielsetzung

Ziel des Bausteins ist es, die Verbindung der Anforderungen des Datenschutzes, die durch das Standard-Datenschutzmodell operationalisiert werden, zum IT-Grundschutz darzustellen.

1.3. Abgrenzung und Modellierung

Der Baustein CON.2 *Datenschutz* ist für den Informationsverbund einmal anzuwenden, wenn personenbezogene Daten unter deutschem oder europäischem Recht verarbeitet werden. Der Baustein CON.2 *Datenschutz* und insbesondere die umfangreichen Erläuterungen in der Einleitung unterstützen somit Anwendende in Deutschland und Europa bei der Orientierung, wenn in der Schutzbedarfsfeststellung Komponenten identifiziert werden, bei denen personenbezogene oder -beziehbare Daten verarbeitet oder sonstig genutzt werden. Dabei sollte dann geprüft werden, ob der Baustein nicht nur auf einzelne Informationsverbünde oder Verfahren, sondern auf die gesamte Institution anzuwenden ist.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein CON.2 *Datenschutz* von besonderer Bedeutung.

2.1. Missachtung von Datenschutzgesetzen oder Nutzung eines unvollständigen Risikomodells

Nach der DSGVO ist die Verarbeitung personenbezogener Daten grundsätzlich verboten. Die Verarbeitung dieser Daten ist nur dann rechtmäßig, wenn die Voraussetzungen des Artikels 6 DSGVO erfüllt sind, also beispielsweise eine Einwilligung der betroffenen Person vorliegt oder eine Rechtsvorschrift die Datenverarbeitung erlaubt. Nicht rechtskonform ist eine Verarbeitung z. B. auch dann, wenn eine Institution eine Datenverarbeitung nicht hinreichend zweckbestimmt, den Zweck überdehnt oder gänzlich zweckungebunden durchführt. Dasselbe gilt, wenn die entsprechende Institution die personenbezogenen Daten intransparent oder ohne integritätssichernde Maßnahmen und ohne Eingriffsmöglichkeiten durch Betroffene verarbeitet.

Aus der Sicht des Datenschutzes ist eine Institution, die personenbezogene Daten verarbeitet (beispielsweise erhebt, speichert, übermittelt oder löscht), grundsätzlich ein Risiko für die davon betroffenen Personen. Dieses Risiko besteht auch dann, wenn die Datenverarbeitung einer Institution rechtskonform ausgestaltet ist.

Ein in der Praxis häufig auftretendes Risiko ist der Zugriff auf Daten, die nicht dem Zweck der ursprünglichen Datenverarbeitung dienen. Dabei kann es sich typischerweise um Zugriffe von ausländischen Konzernmüttern, Sicherheitsbehörden, Banken und Versicherungen, öffentlichen Leistungsverwaltungen, IT-Herstellenden und IT-Dienstleistenden oder Forschungsinstitutionen handeln. Oftmals wird in diesen Kontexten nicht geprüft, ob der Zugriff befugt ist, weil beispielsweise eine langjährig eingefahrene Praxis fortgesetzt wird. Eine andere Möglichkeit ist, dass nachrangige Mitarbeitende das persönliche Risiko scheuen, zu hinterfragen, ob eine hinreichende Rechtsgrundlage vorliegt. Ferner werden aus (teilweise) negativen Prüfergebnissen durch eine Rechtsabteilung oder eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten oft seitens der Verantwortlichen keine Konsequenzen gezogen. Ignorieren Verantwortliche Prüf- oder Beratungsergebnisse, so können sich dadurch Fragen zur Haftung ergeben.

Ein weiteres Risiko sowohl für Personen als auch für verantwortliche Institutionen besteht, wenn für rechtmäßig erfolgte Zugriffe auf IT-Dienste oder die Übermittlung von Datenbeständen durch Dritte

keine Standardprozesse vorgesehen sind. Dasselbe gilt, wenn keine Nachweise über die Ordnungsmäßigkeit in Form von Protokollen und Dokumentationen erbracht werden können.

Eine große Gefahr für Personen oder Beschäftigte ist auch eine mangelhafte Datensicherheit. Erwägungsgrund 75 der DSGVO beschreibt die mit der Verarbeitung personenbezogener Daten einhergehenden Risiken und damit die Gefährdungslage durch unbefugten Zugriff wie folgt: „Die Risiken für die Rechte und Freiheiten natürlicher Personen, mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere, können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren, wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln betreffende Daten verarbeitet werden, wenn persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen, wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft."

2.2. Festlegung eines zu niedrigen Schutzbedarfs

Eine weitere Gefahr für Personen bzw. Beschäftigte ist ein falsch angesetzter Schutzbedarf ihrer personenbezogenen Daten. Dieser Schutzbedarf, der typischerweise durch die Institution, die verantwortlich personenbezogene Daten verarbeitet, selbst festgelegt wird, kann aus verschiedenen Gründen falsch oder zu niedrig angesetzt sein:

- Die Institution hat den gegenüber der Informationssicherheit erweiterten Schutzzielkatalog des Datenschutzes nicht berücksichtigt.
- Die Institution hat bei der Schutzbedarfsermittlung nicht zwischen den Risiken für die Umsetzung der Grundrechte der Betroffenen und den Risiken für die Institution unterschieden.
- Die Institution hat zwar die beiden Schutzinteressen unterschieden, aber die Funktionen des Verfahrens und der Schutzmaßnahmen zugunsten der Institution bzw. zu Ungunsten betroffener Personen gestaltet.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins CON.2 *Datenschutz* aufgeführt. Die Institutionsleitung ist dafür verantwortlich, dass die datenschutzrechtlichen Bestimmungen eingehalten werden. Die Umsetzung der zur Sicherstellung des Datenschutzes erforderlichen Maßnahmen kann sie an eine Organisationseinheit delegieren. Hiervon abzugrenzen ist die Rolle der oder des Datenschutzbeauftragten. Zu ihren Aufgaben gemäß Artikel 39 DSGVO gehört es, die Verantwortlichen, die Auftragsverarbeiter und deren jeweilige Mitarbeitende über ihre datenschutzrechtlichen Pflichten zu unterrichten und zu beraten. Ferner gehört es zu ihren Aufgaben, zu überwachen, ob die datenschutzrechtlichen Bestimmungen eingehalten werden. Die Verantwortung für die Wahrung des Datenschutzes verbleibt hingegen bei den Verantwortlichen bzw.

den Auftragsverarbeitern. Der oder die Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der oder die ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Institutionsleitung
Weitere Zuständigkeiten	Datenschutzbeauftragte

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

CON.2.A1 Umsetzung Standard-Datenschutzmodell (B)

Die gesetzlichen Bestimmungen zum Datenschutz (DSGVO, BDSG, die Datenschutzgesetze der Bundesländer und gegebenenfalls einschlägige bereichsspezifische Datenschutzregelungen) MÜSSEN eingehalten werden. Wird die SDM-Methodik nicht berücksichtigt, die Maßnahmen also nicht auf der Basis der Gewährleistungsziele systematisiert und mit dem Referenzmaßnahmen-Katalog des SDM abgeglichen, SOLLTE dies begründet und dokumentiert werden.

3.2. Standard-Anforderungen

Für diesen Baustein sind keine Standard-Anforderungen definiert.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Für diesen Baustein sind keine Anforderungen für einen erhöhten Schutzbedarf definiert.

4. Weiterführende Informationen

4.1. Wissenswertes

Die EU-Datenschutz-Grundverordnung: „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)" (DSGVO) stellt grundlegende, europaweite gesetzliche Anforderungen an die Einhaltung des Datenschutzes.

Das Standard-Datenschutzmodell (SDM) - „Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele" des Arbeitskreises „Technik" der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder bietet eine Methode, um gesetzliche Datenschutzvorschriften umzusetzen.