Bundesamt
für Sicherheit in der
Informationstechnik

CON: Konzepte und Vorgehensweisen

CON.2: Datenschutz

1 Beschreibung

1.1 Einleitung

Aufgabe des Datenschutzes ist es, Personen davor zu schützen, dass sie durch die Nutzung ihrer personenbezogenen Daten durch Dritte in der Ausübung von Grundrechten beeinträchtigt werden. 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 als Schutzziele ausgewiesen sind. Das Standard-Datenschutzmodell (SDM) bietet eine Methode, um diese geforderte Umsetzung von Datenschutzvorschriften auf der Grundlage von sieben Schutz- bzw. Gewährleistungszielen systematisch überwachen zu können.

1.2 Zielsetzung

Ziel des Bausteins ist es, die Verbindung der Anforderungen des Standard-Datenschutzmodells zum IT-Grundschutz darzustellen.

1.3 Abgrenzung und Modellierung

Der Baustein CON.2 *Datenschutz* dient für Anwender in Deutschland zur Orientierung, wenn in der Schutzbedarfsfeststellung Komponenten identifiziert werden, bei denen eine Verarbeitung und sonstige Nutzung personenbezogener oder -beziehbarer Daten erfolgt. Dabei sollte dann geprüft werden, ob der Baustein nicht nur auf einzelne Informationsverbünde oder Verfahren, sondern auf die gesamte Institution anzuwenden ist.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (kurz: Datenschutzkonferenz, DSK) hat mit dem Standard-Datenschutzmodell eine Methode entwickelt, die die in den deutschen und europäischen Rechtsvorschriften genannten technischen und organisatorischen Maßnahmen auf der Basis von Gewährleistungszielen systematisiert. Damit dient das Modell einerseits den für die Datenverarbeitung verantwortlichen Stellen, erforderliche Maßnahmen systematisch zu planen sowie umzusetzen. Es fördert somit die datenschutzgerechte

Ausgestaltung und Organisation von informationstechnischen Verfahren und Applikationen. Andererseits bietet das Modell den Datenschutzbehörden eine Möglichkeit, mit einer einheitlichen Systematik zu einem transparenten, nachvollziehbaren und belastbaren Gesamturteil über ein Verfahren und dessen Komponenten 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 des Betroffenen und dessen 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 Auswahl von Maßnahmen nach dem SDM ist hingegen die Beeinträchtigung maßgeblich, die ein Betroffener durch die Datenverarbeitung der Institution hinnehmen muss.

Vor diesem Hintergrund ist zwischen der Auswahl von Maßnahmen zur Gewährleistung der Informationssicherheit für Institutionen und der Auswahl von Maßnahmen zur Gewährleistung der Betroffenenrechte zu unterscheiden: Die IT-Grundschutz-Methodik dient vorrangig der Informationssicherheit, das Standard-Datenschutzmodell dient der Umsetzung von Betroffenenrechten.

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, IT-Systeme und Prozesse,
- es berücksichtigt die Einordnung von Daten in die drei Schutzbedarfsabstufungen der Informationssicherheit „normal", „hoch" und „sehr hoch" und ergänzt diese um entsprechende Betrachtungen auf der Ebene von Prozessen und IT-Systemen und
- es bietet einen Katalog mit standardisierten Schutzmaßnahmen.

2 Gefährdungslage

Folgende spezifische 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 EU-Datenschutz-Grundverordnung ist die Verarbeitung personenbezogener Daten grundsätzlich verboten. Die Erhebung, Nutzung und Übermittlung dieser Daten ist nur dann zulässig, wenn eine Rechtsvorschrift dies erlaubt oder anordnet, oder wenn Personen zuvor ausdrücklich eingewilligt haben (vergleiche Artikel 6 DSGVO).

Aus der Sicht des Datenschutzes ist eine Institution, die personenbezogene Daten erhebt, nutzt, übermittelt oder empfängt (zusammengefasst: „verarbeitet") grundsätzlich ein Risiko für Personen. Dieses Risiko besteht auch dann, wenn die Datenverarbeitung einer Institution rechtskonform ausgestaltet ist.

Ein demgegenüber noch einmal erhöhtes Risiko besteht für Personen 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.

Eine häufige Gefahr in der Praxis sind Datenzugriffe von Dritten, 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-Herstellern und IT-Dienstleistern oder Forschungsinstitutionen handeln. Oftmals wird in diesen Kontexten nicht geprüft, ob der Zugriff berechtigt ist, beispielsweise weil eine langjährig eingefahrene Praxis fortgesetzt wird. Eine andere Möglichkeit ist, dass nachrangige Mitarbeiter das persönliche Risiko scheuen, das Vorliegen einer hinreichenden Rechtsgrundlage in Frage zu stellen. Ferner werden aus (teilweise) negativen Prüfergebnissen durch eine Rechtsabteilung oder einen Datenschutzbeauftragten oft seitens der Verantwortlichen keine Konsequenzen gezogen.

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

Eine große Gefahr für Personen bzw. 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. Grundsätzlich ist der Datenschutzbeauftragte zuständig dafür, die Einhaltung der Anforderungen der DSGVO zu überwachen (zu Details und Einschränkungen siehe Art. 39 DSGVO). Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Zuständigkeiten	**Rollen**
Grundsätzlich zuständig	Datenschutzbeauftragter
Weitere Zuständigkeiten	

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein CON.2 *Datenschutz* vorrangig erfüllt werden:

CON.2.A1Umsetzung Standard-Datenschutzmodell (B)

Die gesetzlichen Bestimmungen zum Datenschutz (DSGVO, BDSG und LDSG) 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 den Baustein CON.2 *Datenschutz* sind keine Standard-Anforderungen definiert.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Für den Baustein CON.2 *Datenschutz* 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)" stellt grundlegende, europaweite gesetzliche Anforderungen an die Einhaltung des Datenschutzes.

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

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die Kreuzreferenztabelle enthält die Zuordnung von elementaren Gefährdungen zu den Anforderungen. Anhand dieser Tabelle lässt sich ermitteln, welche elementaren Gefährdungen durch

welche Anforderungen abgedeckt sind. Durch die Umsetzung der aus den Anforderungen abgeleiteten Sicherheitsmaßnahmen wird den entsprechenden elementaren Gefährdungen entgegengewirkt. Die Buchstaben in der zweiten Spalte (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit) zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden. Die folgenden elementaren Gefährdungen sind für den Baustein CON.2 *Datenschutz* von Bedeutung.

G 0.18 Fehlplanung oder fehlende Anpassung