Die rechtlichen Normen der DS-GVO lassen sich nicht ohne weiteres technisch und organisatorisch umsetzen. In der datenschutzrechtlichen Beurteilung müssen Juristen und Informatiker deshalb eine gemeinsame Sprache finden, um sicherzugehen, dass diese rechtlichen Anforderungen auch tatsächlich technisch und organisatorisch umgesetzt werden. Hierbei werden sie durch die Gewährleistungsziele unterstützt. Entsprechend ihres Gehalts, ihrer beabsichtigten Wirkung und Zielrichtung werden die Anforderungen (siehe Teil B) den einzelnen Gewährleistungszielen zugeordnet und auf diese Weise strukturiert und gebündelt. Die technische Gestaltung von Verarbeitungstätigkeiten kann sich an diesen auf Umsetzbarkeit hin ausgerichteten Zielen orientieren, so dass die datenschutzrechtlichen Anforderungen über die Gewährleistungsziele in erforderliche technische und organisatorische Maßnahmen transformiert werden können.

Mit dem SDM wird das Ziel verfolgt, Verarbeitungstätigkeiten rechtskonform auszugestalten. Dazu ist es erforderlich, die von der DS-GVO vorgegebenen datenschutzrechtlichen Anforderungen praktisch umzusetzen und somit sowohl die Risiken für die Rechte und Freiheiten Betroffener zu mindern als auch die Sicherheit der Informationsverarbeitung zu gewährleisten. Das übergeordnete Ziel kann nur erreicht werden, wenn bezogen auf die Daten, Systeme und Dienste sowie Prozesse einer Verarbeitungstätigkeit mehrere Anforderungen – teils alternativ, teils kumulativ – durch technische und organisatorische Maßnahmen erfüllt werden. Mit Hilfe der Gewährleistungsziele werden die rechtlichen Anforderungen strukturiert. Der Unterschied zwischen rechtlichen Anforderungen und Gewährleistungszielen liegt vor allem im Grad der Konkretisierung und der Systematisierung.

C1 Gewährleistungsziele des SDM

Die Funktion der Gewährleistungsziele des SDM wurde im Abschnitt A4 bereits erläutert. Nachfolgend werden die Gewährleistungsziele kurz beschrieben, mit deren Hilfe die Anforderungen der DS-GVO systematisiert werden können (siehe Kapitel C2).

C1.1 Datenminimierung

Das Gewährleistungsziel Datenminimierung erfasst die grundlegende datenschutzrechtliche Anforderung, die Verarbeitung personenbezogener Daten auf das dem Zweck angemessene, erhebliche und notwendige Maß zu beschränken. Die Umsetzung dieses Minimierungsgebots hat einen durchgreifenden Einfluss auf Umfang und Intensität des durch die anderen Gewährleistungsziele bestimmten Schutzprogramms. Datenminimierung konkretisiert und operationalisiert im Verarbeitungsprozess den Grundsatz der Notwendigkeit, der von diesem Prozess insgesamt wie auch von jedem seiner Schritte verlangt, nicht mehr personenbezogene Daten zu verarbeiten, als für das Erreichen des Verarbeitungszwecks benötigt werden. (B1.3 Datenminimierung). Das Minimierungsgebot erstreckt sich dabei nicht nur auf die Menge der verarbeiteten Daten, sondern auch auf den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Insbesondere muss sichergestellt werden, dass personenbezogene Daten nur so lange in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht, wie es für den Zweck der Verarbeitung erforderlich ist (B1.5 Speicherbegrenzung). Datenminimierung reicht vom Design der Informationstechnik durch den Hersteller über ihre Konfiguration und Anpassung an die Betriebsbedingungen (B1.17 Datenschutzfreundliche Voreinstellungen) bis zu ihrem Einsatz in den Kernprozessen der Verarbeitung wie auch in den unterstützenden Prozessen zum Beispiel bei der Wartung der verwendeten Systeme.

C1.2 Verfügbarkeit

Das Gewährleistungsziel Verfügbarkeit bezeichnet die Anforderung, dass der Zugriff auf personenbezogene Daten und ihre Verarbeitung unverzüglich möglich ist und sie ordnungsgemäß im vorgesehenen Prozess verwendet werden können. Dazu müssen sie im Zugriff von Berechtigten liegen und die vorgesehenen Methoden zu deren Verarbeitung müssen auf sie angewendet werden können. Die Verfügbarkeit umfasst die konkrete Auffindbarkeit von Daten z. B. durch Datenmanagement-Systeme, strukturierte Datenbanken und Suchfunktionen und die Fähigkeit der verwendeten technischen Systeme, Daten auch für Menschen angemessen darzustellen (B1.18 Verfügbarkeit). Darüber hinaus müssen zur Umsetzung der Verfügbarkeit Maßnahmen ergriffen werden, die sicherstellen, dass personenbezogene Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können (B1.20 Wiederherstellbarkeit). Es müssen auch Maßnahmen umgesetzt werden, die die Verfügbarkeit der personenbezogenen Daten und der Systeme und Dienste, die diese verarbeiten, garantieren, wenn diese unter einer der Verarbeitung angemessenen zu erwartenden Last stehen und im Falle unerwartet hoher Last sicherstellen, dass der Schutz der personenbezogenen Daten nicht gefährdet ist (B1.19 Belastbarkeit). Sollte in Ausnahmefällen der Schutz personenbezogener Daten bezüglich der Verfügbarkeit dennoch verletzt werden, so ist sicherzustellen, dass Maßnahmen zur Behebung und Abmilderung der Verletzung getroffen werden (B1.23 Behebung und Abmilderung von Datenschutzverletzungen).

C1.3 Integrität

Das Gewährleistungsziel Integrität bezeichnet einerseits die Anforderung, dass informationstechnische Prozesse und Systeme die Spezifikationen kontinuierlich einhalten, die zur Ausübung ihrer zweckbestimmten Funktionen für sie festgelegt wurden (B1.6 Integrität). Integrität bezeichnet andererseits die Eigenschaft, dass die zu verarbeitenden Daten unversehrt (B1.6 Integrität), vollständig, richtig und aktuell (B1.4 Richtigkeit) bleiben. Abweichungen von diesen Eigenschaften müssen ausgeschlossen werden oder zumindest feststellbar sein (B1.22 Überwachung der Verarbeitung), damit sie berücksichtigt und korrigiert werden können (B1.23 Behebung und Abmilderung von Datenschutzverletzungen). Dies gilt auch dann, wenn die unterliegenden Systeme und Dienste unerwartet hoher Last unterliegen (B1.19 Belastbarkeit). Neben dem Aspekt der Fehlerfreiheit muss gerade bei automatisierten Bewertungs- und Entscheidungsprozessen der Aspekt der Diskriminierungsfreiheit gewahrt werden (B1.16 Fehler- und Diskriminierungsfreiheit). Die Faktoren und Eigenschaften eines Bewertungs- oder Entscheidungsprozesses, die potenziell diskriminierende Wirkungen entfalten können, sind a priori im Rahmen der rechtlichen Prüfung festzustellen, bei der Umsetzung zu berücksichtigen und im Betrieb zu überwachen. Dieser Aspekt schlägt sich zum Beispiel durch Maßnahmen zur Bereinigung von Trainingsdaten und der Validierung von Ergebnissen bei der Anwendung von KI-Verfahren nieder.

C1.4 Vertraulichkeit

Das Gewährleistungsziel Vertraulichkeit bezeichnet die Anforderung, dass keine unbefugte Person personenbezogene Daten zur Kenntnis nehmen oder nutzen kann (B1.7 Vertraulichkeit). Unbefugte sind nicht nur Dritte außerhalb der verantwortlichen Stelle, sondern auch Beschäftigte von technischen Dienstleistern, die zur Erbringung der Dienstleistung keinen Zugriff zu personenbezogenen Daten benötigen, oder Personen in Organisationseinheiten, die keinerlei inhaltlichen Bezug zu einer Verarbeitungstätigkeit oder zu der oder dem jeweiligen Betroffenen

haben. Die Vertraulichkeit personenbezogener Daten ist auch dann sicherzustellen, wenn die unterliegenden Systeme und Dienste unerwartet hoher Last unterliegen (B1.19 Belastbarkeit). Sollte in Ausnahmefällen die Vertraulichkeit dennoch verletzt werden, so ist sicherzustellen, dass Maßnahmen zur Behebung und Abmilderung der einhergehenden Verletzung des Schutzes personenbezogener Daten getroffen werden (B1.23 Behebung und Abmilderung von Datenschutzverletzungen).

C1.5 Nichtverkettung

Das Gewährleistungsziel Nichtverkettung bezeichnet die Anforderung, dass personenbezogene Daten nicht zusammengeführt, also verkettet werden. Sie ist insbesondere dann faktisch umzusetzen, wenn die zusammenzuführenden Daten für unterschiedliche Zwecke erhoben wurden (B1.2 Zweckbindung). Je größer und aussagekräftiger Datenbestände sind, umso größer können die Begehrlichkeiten sein, die Daten über die ursprüngliche Rechtsgrundlage hinaus zu nutzen. Rechtlich zulässig sind derartige Weiterverarbeitungen nur unter eng definierten Umständen. Die Nichtverkettung soll durch technische und organisatorische Maßnahmen sichergestellt werden. Neben der Pseudonymisierung sind hierfür auch Maßnahmen geeignet, mit denen die Weiterverarbeitung organisations- bzw. systemseitig getrennt von der Ursprungsverarbeitung geschieht. Der Datenbestand kann bspw. durch Berechtigungssysteme und Reduzierung auf den für den neuen Zweck erforderlichen Umfang angepasst werden.

C1.6 Transparenz

Das Gewährleistungsziel Transparenz bezeichnet die Anforderung, dass in einem unterschiedlichen Maße sowohl Betroffene (B1.1 Transparenz für Betroffene), als auch die Betreiber von Systemen (B1.22 Überwachung der Verarbeitung) sowie zuständige Kontrollinstanzen (B1.8 Rechenschafts- und Nachweisfähigkeit) erkennen können, welche Daten wann und für welchen Zweck bei einer Verarbeitungstätigkeit erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wer die rechtliche Verantwortung für die Daten und Systeme in den verschiedenen Phasen einer Datenverarbeitung besitzt. Transparenz ist für die Beobachtung und Steuerung von Daten, Prozessen und Systemen von ihrer Entstehung bis zu ihrer Löschung erforderlich und eine Voraussetzung dafür, dass eine Datenverarbeitung rechtskonform betrieben und in diese, soweit erforderlich, von betroffenen Personen informiert eingewilligt werden kann (B2 Einwilligungsmanagement). Transparenz der gesamten Datenverarbeitung und der beteiligten Instanzen kann dazu beitragen, dass insbesondere betroffene Personen und Kontrollinstanzen Mängel erkennen und ggf. entsprechende Änderungen an der Verarbeitung einfordern können.

C1.7 Intervenierbarkeit

Das Gewährleistungsziel Intervenierbarkeit bezeichnet die Anforderung, dass den betroffenen Personen die ihnen zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung (B1.11 Berichtigungsmöglichkeit von Daten), Löschung (B1.12 Löschbarkeit von Daten), Einschränkung (B1.13 Einschränkbarkeit der Verarbeitung von Daten), Datenübertragbarkeit (B1.14 Datenübertragbarkeit), Widerspruch und Erwirkung des Eingriffs in automatisierte Einzelentscheidungen (B1.15 Eingriffsmöglichkeit in Prozesse automatisierter Entscheidungen) bei Bestehen der gesetzlichen Voraussetzungen unverzüglich und wirksam gewährt werden (B1.10

Unterstützung bei der Wahrnehmung von Betroffenenrechten) und die verarbeitende Stelle verpflichtet ist, die entsprechenden Maßnahmen umzusetzen. Soweit der Verantwortliche über Informationen verfügt, die es ihm erlauben, die betroffenen Personen zu identifizieren, muss er auch Maßnahmen zur Identifizierung und Authentifizierung der betroffenen Personen, die ihre Rechte wahrnehmen möchten, treffen (B1.9 Identifizierung und Authentifizierung). Zur Umsetzung der Betroffenenrechte und aufsichtsbehördlicher Anordnungen (B3 Umsetzung aufsichtsbehördlicher Anordnungen) sowie der Behebung und Abmilderung von Datenschutzverletzungen (B1.23 Behebung und Abmilderung von Datenschutzverletzungen) müssen die für die Verarbeitungsprozesse Verantwortlichen jederzeit in der Lage sein, in die Datenverarbeitung vom Erheben bis zum Löschen der Daten einzugreifen. Sollte sich die Verarbeitung personenbezogener Daten auf die Einwilligung der betroffenen Person stützen, müssen Maßnahmen ergriffen werden, die sicherstellen, dass die personenbezogenen Daten nur verarbeitet werden, wenn eine Einwilligung der betroffenen Person vorliegt und diese nicht widerrufen wurde (B2 Einwilligungsmanagement).

Für informationstechnische Verarbeitungen, auf die betroffene Personen selbst Zugriff haben (z. B. Anwendungen auf dem Smartphone) und für die unterschiedliche Datenschutzeinstellungen vorgesehen sind, sind durch den Verantwortlichen datenschutzfreundliche Voreinstellungen (Data Protection by Default) festzulegen und weitere Maßnahmen zu treffen. Diese weiteren Maßnahmen müssen die Betroffenen in die Lage versetzen, Konfigurationen differenziert nach den jeweiligen Verarbeitungszwecken selbst vorzunehmen und zu entscheiden, welche Verarbeitungen sie gestatten wollen, die über das erforderliche Minimum hinausgehen (B1.17 Datenschutzfreundliche Voreinstellungen).

C2 Systematisierung der rechtlichen Anforderungen mit Hilfe der Gewährleistungsziele

Im folgenden Abschnitt werden alle im Abschnitt B2 aufgeführten datenschutzrechtlichen Anforderungen der DS-GVO den in Abschnitt C2 beschriebenen Gewährleistungszielen des SDM zugeordnet. Diese Zuordnung dient der in Abschnitt A4 erläuterten Systematisierung der Anforderungen der DS-GVO in Bezug auf die technische und organisatorische Ausgestaltung von Verarbeitungstätigkeiten.

Nr.	Anforderungen der DS-GVO	Gewährleistungsziel
B1.1	Transparenz für Betroffene (Art. 5 Abs. 1 lit a, Art. 12 Abs. 1 und 3 bis Art. 15, Art. 34 DS-GVO)	Transparenz
B1.2	Zweckbindung (Art. 5 Abs. 1 lit. b DS-GVO)	Nichtverkettung
B1.3	Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO)	Datenminimierung
B1.4	Richtigkeit (Art. 5 Abs. 1 lit. d DS-GVO)	Integrität
B1.5	Speicherbegrenzung (Art. 5 Abs. 1 lit. e DS-GVO)	Datenminimierung
B1.6	Integrität (Art. 5 Abs. 1 lit. f, Art. 32 Abs. 1 lit. b, DS-GVO)	Integrität
B1.7	Vertraulichkeit (Art. 5 Abs. 1 lit. f, Art. 28 Abs. 3 lit. b, Art. 29, Art. 32 Abs. 1 lit. b, Art. 32 Abs. 4, Art. 38 Abs. 5 DS-GVO)	Vertraulichkeit

Nr.	Anforderungen der DS-GVO	Gewährleistungsziel
B1.8	Rechenschafts- und Nachweisfähigkeit (Art. 5 Abs. 2, Art. 7 Abs. 1, Art. 24 Abs. 1, Art 28 Abs. 3 lit. a, Art. 30, Art. 33 Abs. 5, Art. 35, Art. 58 Abs. 1 lit. a und lit. e DS-GVO)	Transparenz
B1.9	Unterstützung bei der Wahrnehmung von Betroffenenrechten (Art. 12 Abs. 2 DS-GVO)	Intervenierbarkeit
B1.10	Identifizierung und Authentifizierung (Art. 12 Abs. 6 DS-GVO)	Intervenierbarkeit
B1.11	Berichtigungsmöglichkeit von Daten (Art. 5 lit. d, Art. 16 DS-GVO)	Intervenierbarkeit
B1.12	Löschbarkeit von Daten (Art. 17 Abs. 1 DS-GVO)	Intervenierbarkeit
B1.13	Einschränkbarkeit der Verarbeitung von Daten (Art. 18 DS-GVO)	Intervenierbarkeit
B1.14	Datenübertragbarkeit (Art. 20 Abs. 1 DS-GVO)	Intervenierbarkeit
B1.15	Eingriffsmöglichkeit in Prozesse automatisierter Entscheidungen (Art. 22 Abs. 3 DS-GVO)	Intervenierbarkeit
B1.16	Fehler- und Diskriminierungsfreiheit beim Profiling (Art. 22 Abs. 3, 4 i. V. m. ErwGr. 71)	Integrität
B1.17	Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)	Datenminimierung, Intervenierbarkeit
B1.18	Verfügbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)	Verfügbarkeit
B1.19	Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)	Verfügbarkeit, Integrität, Vertraulichkeit
B1.20	Wiederherstellbarkeit (Art. 32 Abs. 1 lit. b, lit. c DS-GVO)	Verfügbarkeit
B1.21	Evaluierbarkeit (Art. 32 Abs. 1 lit. d DS-GVO).	Sie ist als ein Prozess umzusetzen, der alle Anforderungen umfasst (siehe Kap. D4 Datenschutzmanagement mit dem SDM).
B1.22	Überwachung der Verarbeitung (Art. 33 DS-GVO)	Transparenz, Integrität
B1.23	Behebung und Abmilderung von Datenschutzverletzungen (Art. 33 Abs. 3 lit. d, 34 Abs. 2 DS-GVO).	Integrität, Intervenierbarkeit, Vertraulichkeit, Verfügbarkeit
B2	Einwilligungsmanagement (Art. 4 Nr. 11, Art. 7 Abs. 4 DS-GVO)	Transparenz, Intervenierbarkeit
B3	Umsetzung aufsichtsbehördlicher Anordnungen (Art. 58 Abs. 2 lit. f und lit. j)	Intervenierbarkeit