Mit der DS-GVO wird das Datenschutzrecht europaweit einheitlich geregelt. Die Verordnung ist am 25.05.2016 in Kraft getreten und gilt gemäß Art. 99 Abs. 2 DS-GVO seit dem 25.05.2018 unmittelbar in allen EU-Mitgliedstaaten. Für die nationalen Gesetzgeber wurden durch zahlreiche Spezifizierungsklauseln ergänzende Regelungsbefugnisse geschaffen. Jedoch besteht für die DS-GVO ein grundsätzlicher Anwendungsvorrang vor nationalem Recht. Der Kern der Anforderungen der DS-GVO wird in den Grundsätzen der Verarbeitung personenbezogener Daten gemäß Art. 5 DS-GVO festgehalten, die wiederum den Schutzauftrag aus Art. 8 der Charta der Grundrechte der Europäischen Union aufnehmen.

Entsprechend verpflichtet die DS-GVO Verantwortliche und Auftragsverarbeiter dazu, die Verarbeitungsvorgänge und die hierfür eingesetzte Technik im Hinblick auf die Gewährleistung des grundrechtlichen Schutzes der Rechte der Betroffenen auszugestalten (Art. 25, 28 DS-GVO) sowie zur Minderung der entstehenden Risiken, darunter insbesondere den unbefugten Zugriff durch Dritte die dafür angemessenen technischen und organisatorischen Maßnahmen (u.a. Art. 32, 28 Abs. 3 lit. d DS-GVO) auszuwählen, einzusetzen und auf ihre Wirksamkeit zu überprüfen (Art. 32 Abs. 1 lit. d DS-GVO). Der Verantwortliche ist für die Einhaltung der Grundsätze der Verarbeitung nach Art. 5 Abs. 1, 24 DS-GVO verantwortlich und muss deren Einhaltung nachweisen können.

Die DS-GVO verlangt für Verarbeitungen mit voraussichtlich hohem Risiko für die Rechte und Freiheiten natürlicher Personen die Durchführung einer Datenschutz-Folgenabschätzung (DSFA) gemäß Art. 35 DS-GVO. Die DSFA enthält eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und spezifiziert im Ergebnis technische und organisatorische Maßnahmen zur Bewältigung der erwarteten Risiken. Dies schließt gemäß Art. 35 Abs. 7 DS-GVO Garantien, Sicherheitsvorkehrungen und Verfahren ein, durch die der Schutz personenbezogener Daten sichergestellt, nachgewiesen und überprüft werden kann. Das SDM soll dazu beitragen, die in Art. 5 DS-GVO formulierten Grundsätze für die Verarbeitung personenbezogener Daten umzusetzen und mit überschaubarem Aufwand die von der DS-GVO geforderten Umsetzungsnachweise, bspw. gemäß Art. 5 Abs. 2, Art. 24 Abs. 1 DS-GVO zu erbringen.

Mit dem SDM wird das Ziel verfolgt, die von der DS-GVO vergebenen datenschutzrechtlichen Anforderungen praktisch umzusetzen. Daher ist es erforderlich, aus den gesamten Vorschriften der DS-GVO diejenigen rechtlichen Anforderungen systematisch herauszuarbeiten, die durch technische und organisatorische Maßnahmen zu erfüllen sind. Dies ist erstens mit der Schwierigkeit verbunden, dass diese Anforderungen über die gesamte DS-GVO verstreut und nicht an einer Stelle gebündelt worden sind. Zweitens besteht das Problem, dass die Anforderungen der DS-GVO keinen einheitlichen Konkretisierungsgrad aufweisen. Teilweise formuliert die Verordnung bereits konkrete Anforderungen wie insbesondere in Art. 5 Abs. 1 DS-GVO Transparenz, Datenminimierung und Zweckbindung. Teilweise müssen die rechtlichen Anforderungen aber erst aus den Rechten, Pflichten und sonstigen Vorgaben abgeleitet werden. Häufig ist daher ein Zwischenschritt vom Gesetzestext zur Anforderung erforderlich, wie bei der Vorgabe datenschutzfreundliche Voreinstellungen.

Das SDM legt die folgenden datenschutzrechtlichen Anforderungen zugrunde, die aus der DS-GVO systematisch herausgearbeitet worden sind. Die Anforderungen werden in die drei Blöcke zentrale datenschutzrechtliche Anforderungen, Einwilligungsmanagement und Umsetzung aufsichtsbehördlicher Anforderungen differenziert. Die zentralen datenschutzrechtlichen Anforderungen sind grundsätzlich bei jeder Verarbeitung personenbezogener Daten umzusetzen. Im Einwilligungsmanagement werden die Anforderungen zusammengefasst, die zusätzlich zu erfüllen sind, wenn die Rechtmäßigkeit der Verarbeitung auf Art. 6 Abs. 1 lit. a DS-GVO gestützt wird. Schließlich müssen gegebenenfalls für die Umsetzung aufsichtsbehördlicher Maßnahmen weitere Anforderungen berücksichtigt werden.

Im Folgenden wird übersichtlich dargestellt, aus welchen Vorschriften der DS-GVO welche Anforderungen abgeleitet wurden. [1)]

Die folgenden Anforderungen ergeben sich unmittelbar aus Art. 5 Abs. 1 DS-GVO:

- Transparenz für Betroffene von Verarbeitungen personenbezogener Daten (Art. 5 Abs. 1 lit. a DS-GVO),
- Zweckbindung einer Verarbeitung personenbezogener Daten (Art. 5 Abs. 1 lit. b DS- GVO),
- Datenminimierung einer Verarbeitung personenbezogener Daten (Art. 5 Abs. 1 lit. c DS-GVO),
- Richtigkeit personenbezogener Daten (Art. 5 Abs. 1 lit. d DS-GVO),
- Speicherbegrenzung personenbezogener Daten (Art. 5 Abs. 1 lit. e DS-GVO),
- Integrität personenbezogener Daten (Art. 5 Abs. 1 lit. f DS-GVO, Art. 32 Abs. 1 lit. b DS-GVO),
- Vertraulichkeit personenbezogener Daten (Art. 5 Abs. 1 lit. f DS-GVO, Art. 32 Abs. 1 lit. b DS-GVO),

Übergreifend ergibt sich die Vorgabe, dass der Verantwortliche die Einhaltung des Absatzes 1 nachweisen können muss.

- Rechenschafts- und Nachweisfähigkeit (Art. 5 Abs. 2, Art. 24 Abs. 1 DS-GVO).

Die DS-GVO erkennt verschiedene Rechte der Betroffenen an. Die Rechte der Betroffenen ergeben sich explizit aus Kapitel III der DS-GVO (Art. 12-23 DS-GVO). Der Verantwortliche muss gemäß Art. 12, 24 DS-GVO die Voraussetzungen für die Gewährung dieser Rechte durch technische und organisatorische Maßnahmen schaffen. Aus der rechtlichen Vorgabe der Berücksichtigung der Betroffenenrechte ergeben sich im Einzelnen die folgenden Anforderungen [2)]:

- Unterstützung bei der Wahrnehmung von Betroffenenrechten (Art. 12 Abs. 1 und Abs. 2 DS-GVO,
- Identifizierung und Authentifizierung des Auskunftsersuchenden (Art. 12 Abs. 6 DS- GVO),
- Berichtigungsmöglichkeiten von Daten (Art. 16 DS-GVO),
- Löschbarkeit von Daten (Art. 17 Abs. 1 DS-GVO),
- Einschränkbarkeit der Verarbeitung von Daten (ehemals Sperrung, Art. 18 DS-GVO),
- Datenübertragbarkeit (Art. 20 DS-GVO),
- Eingriffsmöglichkeit in Prozesse automatisierter Entscheidungen (Art. 22 Abs. 3 DS-GVO),
- Fehler- und Diskriminierungsfreiheit beim Profiling (Art. 22 Abs. 3 und 4, Erwägungsgrund 71).

Durch die DS-GVO wird der Datenschutz durch Technik stark gefördert. Dieses wird in Art. 25 und 32 DS-GVO bereits zu mehreren Anforderungen ausdifferenziert:

- Datenschutz durch Voreinstellungen (Art. 25 Abs. 2 DS-GVO),
- Verfügbarkeit der Systeme, Dienste und Daten (Art. 32 Abs. 1 lit. b und lit. c DS-GVO),
- Belastbarkeit der Systeme und Dienste (Art. 32 Abs. 1 lit. b DS-GVO),
- Wiederherstellbarkeit der Daten und des Datenzugriffs (Art. 32 Abs. 1 lit. c DS-GVO),
- Evaluierbarkeit (Art. 32 Abs. 1 lit. d DS-GVO).

Gegenüber Aufsichtsbehörden und Betroffenen besteht für Verantwortliche gemäß Art. 33 und 34 DS-GVO eine Meldepflicht bzw. Benachrichtigungspflicht beim Auftreten von Verletzungen des Schutzes personenbezogener Daten (Datenschutzverletzungen). Daraus ergeben sich Anforderungen an einen ordnungsgemäßen Umgang mit Datenpannen. Dies verlangt die Fähigkeiten zur Feststellung von Datenschutzverletzungen (vgl. Erwägungsgrund 87 DS-GVO), Klassifikation von Datenschutzverletzungen, Meldung von Datenschutzverletzungen an Aufsichtsbehörden (Art. 33 DS-GVO) und Benachrichtigung der Betroffenen von Datenschutzverletzungen (Art. 34 DS-GVO). Daraus

resultieren die Anforderungen:

- angemessene Überwachung der Verarbeitung (Art. 32, 33, 34 DS-GVO)
- Behebung und Abmilderung von Datenschutzverletzungen (Art. 33, 34 DS-GVO).

Beruht die Verarbeitung auf einer Einwilligung, dann sind zusätzlich zu den allgemeinen Anforderungen die spezifischen Anforderungen gemäß Art. 7 und ggfs. Art. 8 DS-GVO einzuhalten (siehe B2).

- Einwilligungsmanagement (Art. 4 Nr. 11, Art. 7 und 8 DS-GVO).

Die DS-GVO räumt Aufsichtsbehörden in Art. 58 DS-GVO verschiedene Befugnisse im Rahmen ihrer Aufgabenerfüllung ein (siehe Kapitel B3):

- Umsetzung aufsichtsbehördlicher Anordnung (Art. 58 DS-GVO).

Die Reihenfolge der folgenden Abschnitte orientiert sich an der Reihenfolge, in der die Anforderungen in der DS-GVO formuliert sind.

B1 Zentrale datenschutzrechtliche Anforderungen der DS-GVO

B1.1 Transparenz für Betroffene

Der Grundsatz der Transparenz ist in Art. 5 Abs. 1 lit. a DS-GVO festgeschrieben. Er findet sich als tragender Grundsatz des Datenschutzrechts in zahlreichen Regelungen der DS-GVO. Insbesondere die Informations- und Auskunftspflichten gemäß Art. 12 ff. DS-GVO tragen ihm Rechnung. In Art. 12 Abs. 1 S. 1 DS-GVO wird gefordert, dass der Verantwortliche geeignete Maßnahmen trifft, um der betroffenen Person alle Informationen bezüglich der Informationspflichten aus Art. 13 und 14 DS-GVO und alle Mitteilungen gemäß den Art. 15 bis 22 und 34 DS-GVO, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Die Betroffenen müssen unverzüglich und auf jeden Fall innerhalb eines Monats über den Stand der Bearbeitung und der ergriffenen Maßnahmen bezüglich ihres Antrags gemäß Art. 12 Abs. 3 DS-GVO informiert werden. Die Benachrichtigungspflicht gemäß Art. 34 DS-GVO bei einer Verletzung des Schutzes personenbezogener Daten, einer sogenannten Datenpanne, dienen dem Grundsatz der Transparenz.

B1.2 Zweckbindung

Die Verpflichtung, Daten nur für den Zweck zu verarbeiten, zu dem sie erhoben wurden, ist insbesondere den einzelnen Verarbeitungsbefugnissen zu entnehmen, die die Geschäftszwecke, die Forschungszwecke etc. zum Maßstab machen und findet über den Zweckbindungsgrundsatz aus Art. 5 Abs. 1 lit. c DS-GVO Eingang in die Grundverordnung. Eine darauf folgende Verarbeitung für weitere Zwecke muss mit dem ursprünglichen Zweck kompatibel sein und die Umstände der Verarbeitung berücksichtigen (Art. 6 Abs. 4 DS-GVO). Über eine Weiterverarbeitung über den ursprünglichen Zweck hinaus, sind die betroffenen Personen ggfs. zu informieren, die von ihrem unter Umständen bestehenden Widerspruchsrecht Gebrauch machen können.

B1.3 Datenminimierung

In einem engen Zusammenhang mit dem Grundsatz der Zweckbindung steht der Grundsatz der Datenminimierung. Der Gesetzgeber fordert, dass personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein müssen (Art. 5 Abs. 1 lit. c DS-GVO). Diese grundlegende Anforderung entspricht weitgehend dem aus dem deutschen Recht bekannten Grundprinzip der Datensparsamkeit. Es ist nur bedingt möglich, zwischen den drei Voraussetzungen dem Zweck angemessen, für den Zweck erheblich und für die Zwecke der Verarbeitung auf das notwendige Maß beschränkt zu differenzieren.

Angemessen sind Daten, die einen konkreten inhaltlichen Bezug zum Verarbeitungszweck aufweisen. Es soll eine wertende Entscheidung über die Zuordnung von Datum und Zweck vorgenommen werden.

Erheblich sind Daten, deren Verarbeitung einen Betrag zur Zweckerreichung leisten. Dieses Merkmal entspricht der Geeignetheit bei der Verhältnismäßigkeitsprüfung. Auf das notwendige Maß beschränkt sind nur die Daten, die zur Erreichung des Zwecks erforderlich sind, ohne deren Verarbeitung der Verarbeitungszweck also nicht erreicht werden kann. Diese Definition ergibt sich auch aus Erwägungsgrund 39. Die Verarbeitung personenbezogener Daten ist demnach nur dann erforderlich, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann. Der Eingriff in das Grundrecht auf Datenschutz ist nur zulässig, soweit er auf das geringstmögliche Maß begrenzt ist.

Die Erforderlichkeit ist ein allgemeiner Grundsatz des Unionsrechts, der durch den Europäischen Gerichtshof (EuGH) in jahrelanger Rechtsprechung anerkannt und ausgeprägt worden ist. Die Vorgabe, nur erforderliche Daten zu verarbeiten, wird in der DS-GVO von dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. b DS-GVO) erfasst. Sie wird zudem als Voraussetzung unmittelbar in den Erlaubnisvorschriften gemäß Art. 6 Abs. 1 S. 1 lit. b bis f und Art. 9 Abs. 2 lit. b, c, f bis j DS-GVO gefordert. Der Grundsatz der Datenminimierung ist nicht nur vor dem Beginn der Verarbeitung zu berücksichtigen, sondern auch fortlaufend. So kann die Anforderung der Beschränkung auf das notwendige Maß dazu führen, dass personenbezogene Daten zu einem bestimmten Zeitpunkt zu anonymisieren sind.

Der Grundsatz der Datenminimierung geht davon aus, dass der beste Datenschutz darin besteht, wenn keine oder möglichst wenige personenbezogene Daten verarbeitet werden. Das Optimierungsziel ist mit dem Bewertungskriterium der Minimierung von Verfügungsgewalt und Kenntnisnahme gegeben. An ihm orientiert kann die optimale Abfolge von Verarbeitungsschritten gewählt und in der Folge an sich verändernde Bedingungen angepasst werden. Im Laufe der Verarbeitung ist schließlich mit technischen und organisatorischen Maßnahmen zu gewährleisten, dass sich die Datenverarbeitung nur innerhalb des a priori gesteckten Rahmens bewegt.

Die frühestmögliche Löschung nicht weiter benötigter und damit nicht mehr erforderlicher personenbezogener Daten ist eine solche Maßnahme. Zuvor jedoch können bereits einzelne Datenfelder oder Attribute von bestimmten Formen der Verarbeitung ausgenommen oder die Zahl der Datensätze, auf die eine Funktionalität anwendbar ist, beschränkt werden. Datenfelder, welche die Identifizierung der Betroffenen ermöglichen, können gelöscht oder transformiert (Anonymisierung, Pseudonymisierung) oder ihre Anzeige in Datenmasken unterdrückt werden, so dass sie den handelnden Personen nicht zur Kenntnis gelangen, vorausgesetzt, diese Kenntnis ist für den jeweiligen Verarbeitungszweck entbehrlich.

B1.4 Richtigkeit

Art. 5 Abs. 1 lit. d DS-GVO formuliert die Anforderung der Richtigkeit personenbezogener Daten. Dies bedingt, dass die von einer Verarbeitung betroffenen personenbezogenen Daten sachlich richtig und erforderlichenfalls auf dem neusten Stand sein müssen. Um diese Anforderung sicherzustellen, sind gemäß der Vorschrift alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten , die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtig werden.

B1.5 Speicherbegrenzung

Der Grundsatz der Speicherbegrenzung wird in Art. 5 Abs. 1 lit. e DS-GVO dahingehend definiert, dass personenbezogene Daten nur so lange in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Hieraus leitet sich die Notwendigkeit von Maßnahmen der Pseudonymisierung, Anonymisierung bzw. Löschung ab. Darüber hinaus wird eine Ausnahme von diesem Grundsatz formuliert, die sich auf die Verarbeitung personenbezogener Daten ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke richtet. Allerdings greift diese Ausnahme nur unter dem Vorbehalt, dass geeignete technische und organisatorische Maßnahmen getroffen werden, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person insbesondere zur Durchsetzung von Zweckbindung und Vertraulichkeit gefordert werden.

B1.6 Integrität

Die Anforderung der Integrität ist in Art. 5 Abs. 1 lit. f DS-GVO als Grundsatz für die Verarbeitung von personenbezogenen Daten und in Art. 32 Abs. 1 lit. b DS-GVO angewendet auf Systeme und Dienste als Aspekt der zu gewährleistenden Sicherheit der Datenverarbeitung genannt. So sind u. a. unbefugte Veränderungen und Entfernungen ausschließen. Personenbezogene Daten dürfen nur in einer Weise verarbeitet werden, die einen Schutz vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen gewährleistet. Es sollen jegliche Veränderungen an den gespeicherten Daten durch unberechtigte Dritte ausgeschlossen oder zumindest so erkennbar gemacht werden, dass sie korrigiert werden können.

B1.7 Vertraulichkeit

Die Verpflichtung zur Wahrung der Vertraulichkeit personenbezogener Daten ergibt sich aus Art. 5 Abs. 1 lit. f DS-GVO. In Bezug auf die zur Verarbeitung eingesetzten Systeme und Dienste sowie für die Auftragsverarbeiter und die Personen, die dem Verantwortlichen oder dem Auftragsverarbeiter unterstellt sind, ergibt sie sich aus Art. 32 Abs. 1 lit. b DS-GVO. Ferner ergibt sie sich aus der Bindung an die Weisungen des Verantwortlichen (Art. 29, 32 Abs. 4 DS-GVO), einer gesonderten Vertraulichkeitsverpflichtung gemäß Art. 28 Abs. 3 lit. b DS-GVO und ggf. gesetzlichen Verschwiegenheitspflichten. Für Datenschutzbeauftragte ergibt sie sich zudem aus der Geheimhaltungspflicht nach Art. 38 Abs. 5 DS-GVO. Unbefugte dürfen keinen Zugang zu den Daten haben und weder die Daten noch Geräte, mit denen diese verarbeitet werden, benutzen können (Art.

32 Abs. 1 lit. b DS-GVO, siehe auch ErwGr. 39 Satz 12). Eine Verletzung der Vertraulichkeit ist insbesondere dann anzunehmen, wenn eine Verarbeitung personenbezogener Daten unbefugt erfolgt.

B1.8 Rechenschafts- und Nachweisfähigkeit

Art. 5 Abs. 2 DS-GVO verpflichtet den Verantwortlichen zum Nachweis der Einhaltung der in Art. 5 Abs. 1 DS-GVO formulierten Grundsätze zur Verarbeitung personenbezogener Daten. Art. 24 Abs. 1 S. 1 DS-GVO erweitert diese Pflicht für den Verantwortlichen dahingehend, dass der Verantwortliche insgesamt sicherzustellen und den Nachweis dafür zu erbringen hat, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese umfassenden Rechenschafts- und Nachweispflichten werden an mehreren Stellen in der DS-GVO konkretisiert. Wenn die Verarbeitung personenbezogener Daten auf der Einwilligung der Betroffenen gründet, so ist der Verantwortliche gemäß Art. 7 Abs. 1 DS-GVO dazu verpflichtet, die Einwilligung der Betroffenen nachweisen zu können. Damit die Verarbeitungstätigkeiten des Verantwortlichen oder Auftragsverarbeiters geprüft werden können, fordert Art. 30 DS-GVO die Anlage eines Verzeichnisses von Verarbeitungstätigkeiten, in dem die einzelnen Verarbeitungstätigkeiten beschrieben werden und Verantwortliche insbesondere den Zweck jeder Verarbeitungstätigkeit angeben müssen. Der Verantwortliche ist darüber hinaus dazu verpflichtet, jede Verletzung des Schutzes personenbezogener Daten für eine etwaige Überprüfung einer Datenschutzbehörde gemäß Art. 33 Abs. 5 DS-GVO zu dokumentieren. Der Verantwortliche muss prüfen, ob seine Verarbeitungstätigkeit wahrscheinlich zu einem hohen Risiko für die Betroffenen führen kann. In diesen Fällen muss der Verantwortliche nachweisen können, dass er eine Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO durchgeführt hat.

Gemäß Art. 58 Abs. 1 lit. a und lit. e DS-GVO kann die Aufsichtsbehörde Verantwortliche (und Auftragsverarbeiter) dazu verpflichten, ihr alle zur Erfüllung ihrer Aufgaben erforderlichen Informationen auf Anfrage bereitzustellen. Verantwortliche und Auftragsverarbeiter müssen in der Lage sein, diese Verpflichtungen zu erfüllen. Datenpannen muss der Verantwortliche unter den in Art. 33 DS-GVO geregelten Umständen an die Aufsichtsbehörden melden.

B1.9 Identifizierung und Authentifizierung

Gemäß Art. 12 Abs. 6 DS-GVO kann der Verantwortliche bei begründeten Zweifeln von einer natürlichen Person, die Betroffenenrechte gemäß Art. 15 bis 21 DS-GVO ihm gegenüber ausüben möchte, Informationen anfordern, die zur Bestätigung der Identität der Person erforderlich sind. Daraus ergibt sich die Anforderung, dass der Verantwortliche eine Vorgehensweise zur Authentifizierung von Personen, die die Betroffenenrechte geltend machen, festlegen und umsetzen muss.

B1.10 Unterstützung bei der Wahrnehmung von Betroffenenrechten

Der Verantwortliche muss Betroffenen gemäß Art. 12 Abs. 2 DS-GVO die Ausübung ihrer Rechte nach Art. 15 bis 22 DS-GVO erleichtern. In jedem Fall müssen Anträge von Betroffenen zur Wahrnehmung ihrer Rechte entgegengenommen und geprüft werden. Maßnahmen zur Umsetzung der Betroffenenrechte müssen ausgewählt und umgesetzt werden.

B1.11 Berichtigungsmöglichkeit von Daten

Von dem Grundsatz der Richtigkeit der Daten in Art. 5 Abs. 1 lit. d DS-GVO ist rechtlich die Berichtigungsmöglichkeit von Daten zu unterscheiden. Diese Anforderung ergibt sich unmittelbar aus dem in Art. 16 DS-GVO festgeschriebenen Recht des Betroffenen auf unverzügliche Berichtigung ihn betreffender unrichtiger Daten, das auch von Aufsichtsbehörden gemäß Art. 58 Abs. 2 lit. g DS-GVO eingefordert werden kann. Aus diesem Recht korrespondiert für den Verantwortlichen die Pflicht, bei Vorliegen der Voraussetzungen die Berichtigung faktisch durchzuführen und die Berichtigung unverzüglich vorzunehmen. Soweit dies nicht ohne Weiteres zu realisieren ist, hat der Verantwortliche hierfür geeignete Vorgehensweisen festzulegen (Art. 24, 25 Abs. 1 i. V. m. 5 Abs. 1 lit. d DS- GVO).

B1.12 Löschbarkeit von Daten

Betroffene haben gemäß Art. 17 Abs. 1 DS-GVO das Recht auf Löschen ihrer Daten, sofern die genannten Voraussetzungen erfüllt sind und keine Ausnahme gemäß Art. 17 Abs. 3 DS- GVO vorliegt. Der Verantwortliche ist verpflichtet, die Löschung der Daten unverzüglich vorzunehmen. Die DS-GVO definiert die Löschung nicht. Nicht die Löschungshandlung sondern deren Ergebnis ist rechtlich entscheidend. Eine datenschutzkonforme Löschung muss dazu führen, dass die Daten nicht mehr verarbeitet werden können. Es muss unverzüglich gelöscht werden. Soweit dies nicht ohne weiteres zu realisieren ist, hat der Verantwortliche hierfür geeignete Vorgehensweisen festzulegen (Art. 24, 25 Abs. 1 i. V. m. 5 Abs. 1 lit. e DS-GVO). Aufsichtsbehörden können gemäß Art. 58 Abs. 2 lit. g DS-GVO die Löschung anordnen.

B1.13 Einschränkbarkeit der Verarbeitung von Daten

Art. 18 DS-GVO sieht als Ergänzung der Löschung von Daten die Einschränkung ihrer Verarbeitung als Betroffenenrecht vor. Art. 4 Nr. 3 DS-GVO definiert die Einschränkung der Verarbeitung als Markierung gespeicherter personenbezogener mit dem Ziel, ihre künftige Verarbeitung so einzuschränken, dass sie nur noch unter den in Art. 18 Abs. 2 DS-GVO genannten Bedingungen (mit Einwilligung oder für die dort bestimmten Zwecke) erfolgen. Die Markierung muss eine technische Maßnahme darstellen, durch die faktisch sichergestellt wird, dass die Daten nur noch begrenzt verarbeitet werden können. Die Aufsichtsbehörden können gemäß Art. 58 Abs. 2 lit. g DS-GVO die Einschränkung der Verarbeitung anordnen.

B1.14 Datenübertragbarkeit

Die Datenübertragbarkeit ist ein neu durch die DS-GVO in Art. 20 eingeführtes Betroffenenrecht. Gemäß Art. 20 Abs. 1 DS-GVO hat die betroffene Person das Recht, die betreffenden Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Aus der Vorschrift ergeben sich bereits konkrete Anforderungen, die der zu übermittelnde Datensatz erfüllen muss. Daten gelten als maschinenlesbar, wenn sie in einem Dateiformat vorliegen, das so strukturiert ist, dass Softwareanwendungen die konkreten Daten einfach identifizieren, erkennen und extrahieren können. [3)] Zudem muss das Datenformat „strukturiert“ und „gängig“ sein. In Erwägungsgrund 68 wird ausgeführt, dass das Format „interoperabel“ sein muss. Der Europäische Datenschutzausschuss führt hierzu in dem Arbeitspapier 242 rev. 01 [4)] führt hierzu aus, dass die Interoperabilität als das Ziel zu verstehen sei, das unter anderem mit den Mitteln maschinenlesbarer, strukturierter und gängiger

Daten erreicht werden könne. Zum Verständnis der „Interoperabilität“ verweist sie auf Art. 2 lit. a Beschluss Nr. 922/2009/EG, wo dieser Begriff in folgender Weise definiert wird: „Interoperabilität [ist] die Fähigkeit verschiedener und unterschiedlicher Organisationen zur Interaktion zum beiderseitigen Nutzen und im Interesse gemeinsamer Ziele; dies schließt den Austausch von Informationen und Wissen zwischen den beteiligten Organisationen durch von ihnen unterstützte Geschäftsprozesse mittels Datenaustausch zwischen ihren jeweiligen IKT-Systemen ein.“

B1.15 Eingriffsmöglichkeit in Prozesse automatisierter Entscheidungen

Art. 22 DS-GVO regelt ein zusätzliches Betroffenenrecht bezogen auf automatisierte Verarbeitungen – einschließlich Profiling gemäß Art. 4 Nr. 4 DS-GVO –, die zu rechtsverbindlichen Entscheidungen im Einzelfall führen. Daraus resultiert in bestimmten Fällen gemäß Absatz 3 dieses Artikels, die Pflicht des Verantwortlichen, angemessene Maßnahmen zu treffen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört. Das Recht einzugreifen setzt voraus, dass in Prozesse automatisierter Entscheidungen manuell eingegriffen und eine Entscheidung im Einzelfall korrigiert werden kann.

B1.16 Fehler- und Diskriminierungsfreiheit beim Profiling

In Erwägungsgrund 71 werden die Anforderungen an den Verarbeitungs- und Bewertungsprozess für das Profiling bezogen auf die Wahrung der Rechte und Freiheiten und der berechtigten Interessen der betroffenen Personen, die Art. 22 Abs. 2 lit. b bzw. a und c DS-GVO i. V. m. Art. 22 Abs. 3 DS-GVO vorsehen, konkretisiert. Es ist eine faire und transparente Verarbeitung zu gewährleisten. Daher sind für das Profiling technische und organisatorische Maßnahmen zu treffen, mit denen in geeigneter Weise sichergestellt wird, dass Faktoren, die zu unrichtigen personenbezogenen Daten oder zu Entscheidungen führen, die die betroffene Person diskriminieren, korrigiert werden und das Risiko von Fehlern minimiert wird. Im Ergebnis soll der Datenverarbeitungsprozess fehler- und diskriminierungsfrei sein.

B1.17 Datenschutz durch Voreinstellungen

Art. 25 Abs. 2 DS-GVO sieht eine neue datenschutzrechtliche Verpflichtung des Verantwortlichen zur Umsetzung des Prinzips Datenschutz durch Voreinstellungen (Data Protection by Default) vor. Der Verantwortliche muss geeignete technische und organisatorische Maßnahmen treffen, die sicherstellen, dass durch Voreinstellungen nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Hierzu ist nicht nur die Menge der verarbeiteten Daten zu minimieren, sondern auch der Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Von den Voreinstellungen kann nur dann in Einzelfällen derart abgewichen werden, dass eine umfassendere Datenverarbeitung vorgenommen bzw. eine breitere Zugänglichkeit ermöglicht werden, wenn Umstände dieser Einzelfälle ein Abweichen erfordern oder die jeweilige betroffene Person ein Abweichen explizit wünscht. Der letztgenannte Fall ist von besonderer Bedeutung, wenn die betroffene Person als Nutzer eines informationstechnischen Systems auf dieses Einfluss nehmen kann und ihr die Möglichkeit eingeräumt wird, Verarbeitungsoptionen zu wählen. Falls umfangreichere Verarbeitungsoptionen zur Verfügung stehen, dürfen sie dann nur durch Betroffene eingeschaltet und aktiviert werden können.

B1.18 Verfügbarkeit

Der Grundsatz der Verfügbarkeit ist in Art. 5 Abs. 1 lit. e DS-GVO verankert und zudem in Art. 32 Abs. 1 lit. b und c DS-GVO explizit im Kontext der Sicherheit von Datenverarbeitungen aufgenommen. Er gewährleistet die Verfügbarkeit der Daten zu dem jeweiligen Zweck, solange dieser noch besteht. Der Grundsatz kommt auch zum Tragen bei den Informations- und Auskunftspflichten gemäß Art. 13, 14 und 15 DS-GVO gegenüber den Betroffenen. Für die Umsetzung des Rechts auf Datenübertragbarkeit gemäß Art. 20 DS-GVO ist die Anforderung der Verfügbarkeit ebenso Grundvoraussetzung.

B1.19 Belastbarkeit

Art. 32 Abs. 1 lit. b DS-GVO fordert die Belastbarkeit der Systeme und Dienste. Das Ziel der Belastbarkeit ist bisher weder aus dem Datenschutzrecht bekannt, noch ist es ein klassisches Ziel der IT-Sicherheit und wird auch insbesondere im IT-Grundschutzkatalog des BSI nicht als Schutzziel aufgegriffen. In der englischen Fassung wird der Begriff „resilience“ verwendet, der in der deutschen Literatur der Informatik regelmäßig mit „Widerstandsfähigkeit“ oder „Ausfallsicherheit“ übersetzt wird. In diesem Sinne bedeutet er, dass die zur Verarbeitung verwendeten Systeme und Dienste auch unter widrigen Einflüssen, die insbesondere von Dritten herrühren können, die Eigenschaften aufrecht erhalten, die eine rechtmäßige Verarbeitung gewährleisten.

B1.20 Wiederherstellbarkeit

Art. 32 Abs. 1 lit. c DS-GVO fordert zur Gewährleistung der Sicherheit der Verarbeitung, die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen. Darunter sind sowohl gezielte Angriffe zu fassen, als auch Unfälle und unvorhersehbare Ereignisse, die zum Beispiel durch Naturphänomene hervorgerufen werden. Der Schwerpunkt der zu treffenden Maßnahmen liegt auf dem zeitlichen Aspekt der Wiederherstellbarkeit. Die Vorschrift fordert insofern insbesondere eine prozessorientierte Notfallplanung mit zugeordneten Wiederanlaufzeiten. Insofern geht die Wiederherstellbarkeit der Daten und des Datenzugriffs über die allgemein in Art. 32 Abs. 1 lit. b DS-GVO geforderte Verfügbarkeit hinaus. Der Gesetzgeber geht insofern davon aus, dass für das Ziel der raschen Wiederherstellbarkeit nach einem Zwischenfall zusätzliche technische und organisatorische Maßnahmen zu ergreifen sind.

B1.21 Evaluierbarkeit

Die in Art. 32 Abs. 1 lit. d DS-GVO geforderte Evaluierung dient nicht unmittelbar, sondern mittelbar dem operativen Datenschutz und der Datensicherheit. Es soll ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung entwickelt und umgesetzt werden.

B1.22 Überwachung der Verarbeitung

Um eine wirksame Behebung und Abmilderung sicherstellen zu können, können der Verantwortliche und der Auftragsverarbeiter ggf. dazu verpflichtet sein, als technische und organisatorische

Maßnahme i. S. d. Art. 32 DS-GVO eine Überwachung der Verarbeitung durchzuführen.

B1.23 Behebung und Abmilderung von Datenschutzverletzungen

Der Verantwortliche muss gemäß Art. 33 Abs. 3 lit. d und 34 Abs. 2 DS-GVO bei Datenschutzverletzungen – im Einklang mit Art. 24 und Art. 32 DS-GVO – technische und organisatorische Maßnahmen umsetzen, die die Datenpanne beheben und eventuelle Folgen für die Betroffenen abmildern.

B2 Einwilligungsmanagement

Eine besondere Rechtsgrundlage stellt die in Art. 6 Abs. 1 lit. a in Verbindung mit Art. 4 Nr. 11 DS-GVO geregelte Einwilligung dar. Sofern die Zulässigkeit der Datenverarbeitung auf einer wirksamen Einwilligung basieren soll, ergeben sich aus diesen Vorschriften datenschutzrechtliche Anforderungen an das Einwilligungsmanagement, das das vollständige Verfahren der Einholung, der Speicherung, der Dokumentation, des Nachweises sowie der Umsetzung eines Widerrufs der Einwilligung umfasst. Im Einzelnen ist die Einwilligung nur wirksam, wenn

- eine vorherige umfassende Information des Betroffene über die Datenverarbeitung erfolgt ist,
- der Einwilligungstext konkrete Datenverarbeitungen klar und eindeutig benennt,
- die Einwilligung freiwillig erklärt wird und
- eine unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder

einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, erfolgt.

Schließlich muss ein jederzeitiger Widerruf der Einwilligung möglich sein mit der Konsequenz, dass die personenbezogenen Daten dann nicht mehr weiterverarbeitet und unter Einhaltung gesetzlicher Fristen gelöscht werden.

Art. 7 Abs. 3 DS-GVO schreibt fest, dass der Widerruf einer Einwilligung so einfach sein muss wie ihre Erteilung. Der Verantwortliche hat geeignete Vorgehensweisen für die Entgegennahme und die Umsetzung des Widerrufs festzulegen.

Insbesondere wenn Einwilligungen über elektronische Kommunikationsmittel eingeholt werden, folgen aus diesen rechtlichen Vorgaben Anforderungen an die Ausgestaltung des Verfahrens.

B3 Umsetzung aufsichtsbehördlicher Anordnungen

Art. 58 Abs. 2 lit. f DS-GVO erlaubt Aufsichtsbehörden gegenüber Verantwortlichen die Beschränkung einer Verarbeitung zu verhängen, die dazu führen kann, dass die Verarbeitung nicht in der vorgesehenen Art und Weise fortgesetzt werden darf. Die Beschränkung kann qualitativ oder quantitativ ausgerichtet sein. Als qualitative Beschränkungen können z. B. Anordnungen getroffen werden, dass nur bestimmte Daten oder Daten nur zu bestimmten Zwecken verarbeitet werden dürfen sowie räumliche und zeitliche Verarbeitungsgrenzen festgelegt werden. Als eine quantitative Beschränkung kommt z. B. die Begrenzung von Zugriffsberechtigungen auf Datenbanken in Betracht. Beschränkungen können somit sehr unterschiedlich ausgestattet sein. Aufgrund dieser

Vielgestaltigkeit kann nur die recht abstrakte Anforderung der Umsetzbarkeit aufsichtsbehördlicher Maßnahmen formuliert werden.

Art. 58 Abs. 2 lit. j DS-GVO erlaubt Aufsichtsbehörden anzuordnen, dass eine Übermittlung von Daten an Empfänger in Drittländern ausgesetzt wird. Die Umsetzung dieser Anordnung setzt voraus, dass die Empfänger von personenbezogenen Daten lokalisiert werden können und Datenübermittlungen nach dem Kriterium des Empfängerlandes gesteuert werden können.

---

1) Das SDM betrachtet weder grundlegende Fragen der materiellen Rechtmäßigkeit einer Verarbeitung noch spezialgesetzliche Regelungen oder Regelungen auf einem hohen Detaillierungsgrad. Daher ist aus dieser rechtlichen Vorgabe keine Anforderung abzuleiten, die im SDM aufgenommen wird. Die Orientierung an den allgemein geltenden Grundsätzen des Datenschutzes erübrigt daher nicht die Kenntnisnahme der datenschutzrechtlichen Regelungen, auch nicht im Bereich der technischen und organisatorischen Maßnahmen.

2) Die Prüfung der Voraussetzungen der Betroffenenrechte muss erfolgen, ist aber nicht Gegenstand des SDM.

3) S. EG 21 der RL 2013/37/EU.

4) Dieses Arbeitspapier wurde ursprünglich durch die Vorgängerinstitution des EDSA, die Artikel-29-Arbeitsgruppe, und später durch den EDSA mit Bestätigung 1/2018 angenommen.