# Baustein 61 „Berichtigen“

Version: V1.0
Bezugsquelle: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/

| Versionshistorie | gültig seit | gültig bis |
|---|---|---|
| SDM-V2.0_Berichtigen_V1.0 | 06.10.2020 | |

## 1. Bezug zu den Anforderungen der DS-GVO und den Gewährleistungszielen

Dieser Baustein dient vorrangig der Umsetzung folgender DS-GVO-Anforderungen (vgl. SDM-V2b-Methodik-Handbuch, Teil B):

| Anforderungen der DS-GVO | Gewährleistungsziele |
|---|---|
| Berichtigungsmöglichkeit von Daten (Art. 5 lit. d, Art. 16 DS-GVO) | Intervenierbarkeit |
| Richtigkeit (Art. 5 Abs. 1 lit. d DS-GVO) | Integrität |

## 2. Beschreibung

Verantwortliche müssen angemessene Maßnahmen treffen, um zu gewährleisten, dass gespeicherte personenbezogene Daten im Hinblick auf die Zwecke ihrer Verarbeitung sachlich richtig und erforderlichenfalls auf dem neusten Stand sind (Art. 5 Abs. 1 lit. d DS-GVO). Betroffene Personen haben das Recht, eine Berichtigung ihrer personenbezogenen Daten vom Verantwortlichen zu verlangen, wenn sie unrichtig sind (Art. 16 DS-GVO).

Das Betroffenenrecht zur Berichtigung von Daten (Art. 16 DS-GVO) ergänzt den Grundsatz der Datenrichtigkeit, nach dem Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein müssen (Art. 5 Abs. 1 lit. d DS-GVO) und andernfalls entweder gelöscht (siehe Baustein „Löschen“) oder berichtigt werden müssen.

Der Berichtigungsanspruch besteht selbst dann, wenn nur eine geringfügige Unrichtigkeit vorliegt.

Ein Spezialfall der Berichtigung ist die Vervollständigung (Art. 16 Satz 2 DS-GVO). Unvollständige Daten können dann unrichtig sein, wenn durch das Fehlen bestimmter Angaben ein im Hinblick auf den Verarbeitungszweck falscher Eindruck entstehen könnte.

Die Verwendung von falschen Feld- oder Spaltenbezeichnungen, stellt auch eine Form von unrichtigen personenbezogenen Daten dar. Die Angaben können bspw. dadurch berichtigt werden, indem die Daten unter die richtigen Feldbezeichnungen bzw. unter die richtigen Spaltenbezeichnungen eingeordnet werden oder die Feld- oder Spaltenbezeichnungen selbst angepasst werden.

Werden Daten gespeichert, um Zustände zu bestimmten Zeitpunkten oder einen zeitlichen Verlauf zu dokumentieren, dann ist das entsprechende (mit einem Zeitpunkt verknüpfte) personenbezogene Datum nicht allein deshalb unrichtig, weil es nicht den aktuellen Stand wiedergibt, sondern den Stand zu dem mit ihm verknüpften Zeitpunkt (bspw. bei Einträgen im Grundbuch).

Die Unrichtigkeit kann offenkundig sein, sich aus der Begründung ergeben, mit der eine betroffene Person einen Berichtigungsanspruch geltend macht, oder dem Verantwortlichen durch Hinweise Dritter bekannt werden. Betroffene Personen können Unrichtigkeiten auch erkennen, indem sie ihr Recht auf Auskunft (Art. 15 DS-GVO) wahrnehmen. Das Verlangen der betroffenen Person nach Berichtigung kann ein, muss aber nicht der alleinige Auslösungsfaktor für die Berichtigung sein. Der Verantwortliche MUSS Daten berichtigen, wenn er von deren Unrichtigkeit Kenntnis hat.

Um den Anspruch auf Berichtigung der Daten geltend zu machen, kann die betroffene Person einen Antrag beim Verantwortlichen stellen. Da die Form des Antrags nicht vorgeschrieben ist, MUSS der Verantwortliche Anträge in jeder Form entgegennehmen, wenn er über den entsprechenden Kommunikationskanal erreichbar ist. Der Verantwortliche SOLLTE betroffenen Personen insbesondere die Möglichkeit einräumen, den Antrag schriftlich oder in Textform zu stellen, um die vom Verantwortlichen einzuhaltenden Fristen leichter nachprüfen zu können. Zudem SOLLTE der Verantwortliche dafür sorgen, dass Anträge auch elektronisch gestellt werden können.

Hat der Verantwortliche begründete Zweifel an der Identität der betroffenen Person, kann er zusätzliche Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind (Art. 12 Abs. 6 DS-GVO).

Der Verantwortliche MUSS einen Antrag auf Berichtigung unverzüglich beantworten. Er muss allerdings die Möglichkeit haben, das Vorliegen der Voraussetzungen des Berichtigungsanspruchs zu prüfen. Spätestens innerhalb eines Monats nach Eingang des Antrags MUSS er aber die betroffene Person über die ergriffenen Maßnahmen, über eine mögliche Fristverlängerung zusammen mit den Gründen für die Verzögerung oder über die Ablehnung des Antrags einschließlich der Gründe hierfür informieren (Art. 12 Abs. 3 und 4 DS-GVO). Die betroffene Person kann für die Dauer, die es dem Verantwortlichen ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen, von dem Verantwortlichen die Einschränkung der Verarbeitung verlangen (siehe Baustein „Einschränken der Verarbeitung“). Die eigentliche Berichtigung darf der Verantwortliche nicht länger als unvermeidlich hinauszögern.

Kann die betroffene Person die Unrichtigkeit nachweisen, MUSS der Verantwortliche berichtigen. Kann hingegen der Verantwortliche die Richtigkeit der gespeicherten Daten nachweisen, besteht kein Berichtigungsanspruch. Lässt sich weder die Richtigkeit noch die Unrichtigkeit der Daten nachweisen, ist eine Einschränkung der Verarbeitung gemäß Art. 18 Abs. 1 lit. a DS-GVO, die infolge des Bestreitens der Richtigkeit an sich nur für die Dauer der

Prüfung gilt, fortzusetzen. Die betroffene Person kann nicht verlangen, dass anstelle der gespeicherten unbewiesenen Daten die von der betroffenen Person behaupteten, ebenfalls nicht bewiesenen Daten gespeichert werden.

Lehnt der Verantwortliche die Berichtigung ab, MUSS er dies begründen und auf die weiteren Durchsetzungsmöglichkeiten für die betroffene Person hinweisen, nämlich auf die Beschwerde bei einer Aufsichtsbehörde und auf einen gerichtlichen Rechtsbehelf (Art. 12 Abs. 4 DS-GVO).

Neben der Beantragung der Berichtigung durch die betroffene Person hat die Aufsichtsbehörde die Möglichkeit, gegenüber dem Verantwortlichen die Berichtigung der Daten anzuordnen, etwa im Fall des Vorliegens einer Beschwerde.

Die Ansprüche der betroffenen Person auf Berichtigung oder Vervollständigung personenbezogener Daten würden weitgehend leerlaufen, wenn mögliche Empfänger nicht über Berichtigungen oder Vervollständigungen von Daten informiert werden würden. Der Verantwortliche MUSS deshalb allen Empfängern die Berichtigung oder Vervollständigung von Daten mitteilen, es sei denn dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden (Art. 19 Satz 1 DS-GVO). Diese Benachrichtigung soll es dem Empfänger ermöglichen, die bei ihm zu der betroffenen Person vorhandenen Daten zu prüfen und seinerseits einer möglichen Pflicht zur Berichtigung nachzukommen. Die Mitteilung an die Empfänger setzt in der Regel voraus, dass der Verantwortliche zurückverfolgen kann, welchen Empfängern er welche Daten zuvor offengelegt hat. Um seine Informationspflicht erfüllen zu können, SOLLTE der Verantwortliche jede Art von Offenlegungen protokollieren und diese Protokolle während der gesamten Aufbewahrungsfrist der betreffenden Daten speichern. Im Gegensatz zur Benachrichtigungspflicht gegenüber Empfängern verpflichtet die DS-GVO den Verantwortlichen zwar nicht ausdrücklich, Absender ebenfalls zu unterrichten. Mit Blick auf den Grundsatz der Richtigkeit (Art. 5 Abs. 1 lit. d DS-GVO) SOLLTE der Verantwortliche, wenn er Daten berichtigt hat, dennoch demjenigen die Berichtigung mitteilen, der ihm die (falschen) personenbezogenen Daten zuvor übermittelt hat.

Für den Fall, dass mehrere Verantwortliche gemeinsam verantwortlich sind (Art. 26 DS-GVO), kann die Pflicht zur Berichtigung mehrere Verantwortliche treffen (siehe Abschnitt „Technische Systeme“).

Werden personenbezogene Daten im Auftrag eines Verantwortlichen durch Auftragsverarbeiter verarbeitet, sind die Rechte der betroffenen Personen auf Berichtigung gegenüber dem Verantwortlichen geltend zu machen. Auftragsverarbeiter sind jedoch insofern von der Pflicht zur Berichtigung betroffen, als dass sie den Verantwortlichen ggf. bei erforderlichen Berichtigungen unterstützen müssen.

Falls Daten mehrfach gespeichert sind, müssen auch alle Kopien berichtigt werden (siehe Abschnitt „Technische Systeme“ und weitergehende Anforderungen bei hohem Schutzbedarf).

Einschränkungen der Berichtigungspflicht können sich aus spezialgesetzlichen Regelungen ergeben, die durch entsprechende Öffnungsklauseln bspw. die Verarbeitung personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken (Art. 89 Abs. 2 DS-GVO) oder für im öffentlichen Interesse liegende Archivzwecke (Art. 89 Abs. 3 DS-GVO) ermöglichen. So ist gem. § 27 Abs. 2 BDSG das Recht auf Berichtigung insoweit beschränkt, als diese Rechte voraussichtlich die Verwirklichung der Forschungs- oder Statistikzwecke unmöglich machen oder ernsthaft beinträchtigen und die Beschränkung für die Erfüllung der Forschungs- oder Statistikzwecke notwendig ist. Gemäß § 28 Abs. 3 BDSG besteht das Recht auf Berichtigung auch dann nicht, wenn die personenbezogenen Daten zu Archivzwecken im öffentlichen Interesse verarbeitet werden. Bestreitet die betroffene Person in diesem Kontext die Richtigkeit der personenbezogenen Daten, MUSS ihr die Möglichkeit einer Gegendarstellung eingeräumt werden. Das zuständige Archiv MUSS die Gegendarstellung den Unterlagen hinzuzufügen. Für Landesbehörden ist das Landesrecht zu berücksichtigen, das weitere abweichende Regelungen enthalten kann (bspw. § 11 Abs. 2 LArchivG M-V).

Um Daten wirksam berichtigen zu können, sind Maßnahmen auf der Ebene der Daten, der technischen Systeme und der dazugehörigen Prozesse erforderlich.

Daten

Die Struktur der Daten und das Datenmodell MÜSSEN so organisiert werden, dass einzelne Datenfelder, Datensätze oder Gruppen von Daten berichtigt werden können (M61.D01).

Es MUSS sichergestellt werden, dass im Fall einer Rücksicherung die in Kopien oder Sicherungen nicht berichtigten Daten den aktuellen, berichtigten, Datenbestand nicht „überschreiben“ und somit wieder für die Bearbeitung herangezogen werden (M61.D02).

Um Zeitverläufe dokumentieren zu können, SOLLTEN entsprechende Datenfelder vorgesehen werden (M61.D03). Für die (u. a. in diesem Zusammenhang erforderlichen) Zeitstempel SOLLTEN geeignete Datenfelder bereitgestellt werden (M61.D04). In diesem Zusammenhang sind auch die Anforderungen des Bausteins „Protokollieren“ zu berücksichtigen.

Schließlich sind Datenfelder sinnvoll, in denen identifizierende Daten der betroffenen Person gespeichert werden (M61.D05), um auch nachträglich nachweisen zu können, dass die Berichtigung von Daten nicht unbefugt beantragt wurde.

Technische Systeme

Die technischen Systeme zur Umsetzung der vom Verantwortlichen angeordneten Berichtigung hängen neben dem Schutzbedarf maßgeblich von der Art und Weise des jeweiligen Datenträgers ab, auf dem die Daten gespeichert sind. Die Systeme MÜSSEN in jedem Fall so gestaltet sein, dass die Berichtigungsvorgänge technisch realisiert (M61.S01) oder dass Daten in Zweifelsfällen für die weitere Verarbeitung eingeschränkt werden können (M61.S02).

Die technischen Systeme MÜSSEN in der Lage sein, Berichtigungen durchzuführen, ohne die Integrität des unverändert verbleibenden Datenbestandes zu beeinträchtigen (M61.S03).

Die im Berechtigungs- und Rollenkonzept abgebildeten Berechtigungen MÜSSEN durch ein technisches Zugriffsrechtesystem umgesetzt werden, damit u. a. unbefugte Berichtigungen verhindert oder zumindest nachträglich erkannt werden können (M61.S04).

Da es erforderlich ist, Fristen zur Berichtigung von Daten zu überwachen, SOLLTE der Verantwortliche entsprechende Systeme wie Trouble-Ticket-Systeme vorhalten (M61.S05). Hierfür ist auch der Einsatz von Zeitstempel-Systemen erforderlich (M61.S06).

Es MÜSSEN technische Systeme zur Verfügung stehen, die die betroffenen Personen sicher identifizieren und somit garantieren, dass die Berichtigung von Daten nicht unbefugt beantragt wird und ausschließlich die Daten der beantragenden Person verändert werden (M61.S07).

Damit alle Datenempfänger von erforderlichen Berichtigungen informiert werden können, MUSS der Verantwortliche in der Regel alle Offenlegungen nachvollziehen können, bspw. durch entsprechende Protokollierung werden (M61.S09), siehe auch Baustein „Protokollieren“.

Alle Forderungen in Bezug auf die Berichtigung von Daten MÜSSEN grundsätzlich auch bei allen Kopien und Datensicherungen umgesetzt werden können. Das bedeutet jedoch nicht, dass in jeder Kopie und jedem Backup Daten zum gleichen Zeitpunkt wie im Originaldatenbestand berichtigt werden muss, da das Berichtigen von Daten in Sicherungskopien in der Regel mit einem wesentlich höheren Zeitbedarf als das Berichtigen im aktiven Datenbestand produktiver IT-Systeme und Dienste verbunden ist. Die technischen Systeme zur Rücksicherung von Daten MÜSSEN ermöglichen, dass bei der Wiederherstellung von Daten etwa nach einem Havariefall die vormals berichtigten Daten erneut berichtigt werden, und somit ausgeschlossen wird, dass falsche Daten wieder für die Verarbeitung herangezogen werden (M61.S10).

Prozesse

Der Verantwortliche MUSS in einem Konzept festlegen, wie er die datenschutzrechtlichen Pflichten zur Berichtigung personenbezogener Daten erfüllen will (M61.P01). Dazu gehört auch, dass Prozesse eingerichtet werden, die betroffenen Personen das Recht auf Auskunft einräumen (M61.P02).

Der gesamte Vorgang des Berichtigens SOLLTE von einem auf die jeweilige Verarbeitungstätigkeit zugeschnittenen standardisierten Prozess gesteuert werden, der die einzelnen Berichtigungsschritte beschreibt und so zu weitgehend standardisierten Abläufen führt (M61.P03). Alle Berichtigungsvorgänge müssen dokumentiert werden, u. a. auch der Grund der Berichtigung, siehe Baustein „Dokumentieren“ ( M61.P04).

Haben zwei oder mehr Verantwortliche gemeinsam Zwecke und Mittel der betreffenden Verarbeitungstätigkeit festgelegt, so MÜSSEN sie als gemeinsam Verantwortliche in einer Vereinbarung festlegen, wer von ihnen welche Pflichten im Zusammenhang mit Berichtigungen übernimmt (M61.P05).

Um personenbezogene Daten berichtigen zu können, die von einem Dienstleister im Auftrag verarbeitet werden, MUSS der Verantwortliche die Mitwirkungspflichten des Auftragsverarbeiters im Vertrag gem. Art. 28 Abs. 3 DS-GVO festschreiben (M61.P06).

Damit die Berichtigungsansprüche der betroffenen Person auch in Backups oder Kopien umgesetzt werden können, SOLL der Verantwortliche eine Übersicht über alle angefertigten Kopien und deren Erstellungsdatum führen (M61.P07).

Es ist ein Berechtigungs- und Rollenkonzept erforderlich, auf dessen Basis ein in einem Berichtigungskonzept beschriebener organisatorischer Prozess steuert, welche Personen des Verantwortlichen für die Prüfung, Anordnung und Durchführung von Berichtigung zuständig sind. Da sich das Berichtigen personenbezogener Daten auch auf einen bestimmten Personenkreis bzw. bestimmte Rollen innerhalb und außerhalb der verantwortlichen Stelle beziehen kann, SOLLTEN Berichtigungsprozesse auch rollenabhängig konfigurierbar sein (M61.P08).

Verantwortliche MÜSSEN in der Lage sein, Offenlegungen nachvollziehen zu können, um Datenempfänger über die erfolgten Berichtigungen informieren zu können, sofern sich dies nicht als unmöglich erweist oder mit einem unverhältnismäßigen Aufwand verbunden ist. Dafür sind entsprechende Dokumentationsprozesse erforderlich (M61.P09), deren Daten jedoch für die Nachberichtspflicht zweckgebunden sind.

Um zu überwachen, ob in angemessener Zeit berichtigt wird, MUSS der Verantwortliche über Prozesse zur Fristenüberwachung verfügen (M61.P10).

Der Verantwortliche SOLLTE Antragsformulare bereitstellen, mit denen betroffene Personen die Berichtigung von Daten beantragen können (M61.P11). Der Verantwortliche MUSS sicherstellen, dass er Anträge unabhängig von ihrer Form entgegennimmt, wenn er über den entsprechenden Kommunikationskanal erreichbar ist (M61.P12). Insbesondere SOLLTE der Verantwortliche dafür sorgen, dass Anträge auch elektronisch gestellt werden können (M61.P13). Für den Fall notwendiger Identitätsprüfungen von Antragstellern MUSS der Verantwortliche entsprechende Prozesse zur Identitätsprüfung einrichten (M61.P14). Der Verantwortliche MUSS sicherstellen, dass Anträge unverzüglich, spätestens in den gesetzlichen Fristen bearbeitet werden (M61.P15).

Im Zusammenhang mit der Berichtigung personenbezogener Daten treffen den Verantwortlichen Mitteilungspflichten, die in einem organisatorischen Prozess abgebildet werden müssen (M61.P16). Der Verantwortliche MUSS die Empfänger informieren, denen berichtigte Daten zuvor offengelegt wurden, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden (M61.P17). Zudem SOLLTE er auch die Absender informieren, von denen er zu berichtigende Daten erhalten hat (M61.P18).

Lehnt der Verantwortliche die Berichtigung von Daten ab, MUSS er dies begründen und die betroffene Person auf das Recht zur Beschwerde bei einer Aufsichtsbehörde und auf einen gerichtlichen Rechtsbehelf hinweisen. Es MÜSSEN Vorgaben existieren, wie das Ablehnen unberechtigter Berichtigungswünsche organisiert wird und auf welchem Weg und von wem die betroffene Person informiert wird (M61.P19).

Sofern Berichtigungen – im Rahmen einer unverzüglichen Berichtigung – „im Block“ durchgeführt werden, SOLLTEN entsprechende Prozesse diese Abläufe steuern (M61.P20).

Im Bereich der Speicherung personenbezogener Daten zu Archivzwecken im öffentlichen Interesse MUSS das zuständige Archiv Prozesse bereitstellen, die es betroffenen Personen ermöglichen, eine Gegendarstellung den Unterlagen hinzuzufügen (M61.P21).

## 3. Differenzierung bei hohem Schutzbedarf

Sollen Daten berichtigt werden, deren Verarbeitung zu einem hohen Risiko führt, SOLLTE die Struktur der Daten und das Datenmodell so organisiert werden, dass nicht nur Datensätze oder Gruppen von Daten berichtigt werden können, sondern dass die Berichtigung feingranular auf einzelne Datenfelder bezogen möglich ist (M61.D06). Dies ist regelmäßig erforderlich, um eine schnellstmögliche Korrektur unrichtiger Daten zu gewährleisten und eine weitere Verarbeitung von unrichtigen Daten auszuschließen. Eine feingranulare Struktur der Daten erleichtert zudem die Gewährleistung der Integrität der Daten, die nicht von der Berichtigung betroffen sind, insbesondere dann, wenn die Integrität von Daten mittels zusätzlicher Maßnahmen, wie digitalen Signaturen, geschützt wird.

Werden Unrichtigkeiten bei besonderen Kategorien personenbezogener Daten gemäß Art. 9 DS-GVO festgestellt, muss geprüft werden, ob hier im Einzelfall ein hohes Risiko für die betroffene Person vorliegt. Wenn dies zu bejahen ist, sind die betroffenen Daten schnellstmöglich zu berichtigen.

Hierbei ist zu beachten, dass es gerade im Bereich von ärztlichen Diagnosen und Befundberichten schwierig sein kann, zu beantworten, inwieweit diese einer Korrektur und Berichtigung zugänglich sind. Dies ist jedenfalls im Hinblick auf objektive Umstände anzunehmen, die einem Nachweis zugänglich sind (Zeitpunkt der Untersuchung, Alter/ Größe des Patienten). Bei subjektiven Feststellungen und fachlichen Bewertungen des Behandelnden dürfte es aber regelmäßig der Einbindung eines entsprechenden, externen

Fachgremiums bedürfen (Landesärztekammer, Berufsgericht etc.) bevor hierzu abschließende Feststellungen getroffen werden können.

Sollen Daten berichtigt werden, deren Verarbeitung zu einem hohen Risiko führt, sind auch besondere Anforderungen an den Umgang mit Backups zu stellen. Das Berichtigen kann bei hohem Schutzbedarf das „außerplanmäßige Aufräumen“ von Backups erfordern. Auch ohne das Erfordernis eines Restores müssen in diesem Fall Datenbestände zurückgespielt, teilweise berichtigt und die verbleibenden Daten erneut gesichert werden. Je höher der Schutzbedarf ist, umso höher muss die Frequenz dieser „Korrekturläufe“ sein (M61.P22).

Bei der Berichtigung von Daten, deren Verarbeitung zu einem hohen Risiko führt, sind an die eindeutige Identitätsfeststellung der betroffenen Person besonders hohe Anforderungen zu stellen. Der Verantwortliche SOLLTE die Möglichkeit der Identifizierung mit Hilfe der eID-Funktion des Personalausweises anbieten (M61.S08), einen etablierten Kommunikationskanal mit aktiver Zwei-Faktor-Authentifizierung (M61. S12) oder in geeigneten Fällen notariell beglaubigte Unterschrift oder beglaubigte Kopie des Personalausweises einfordern (M61.P23).

Je höher der Schutzbedarf ist, umso höhere Anforderungen sind auch an die Authentisierung desjenigen zu stellen, der die Berichtigung vornehmen soll. Als Authentifizierungsmerkmal reicht bei hohem Schutzbedarf Wissen allein (bspw. Kennung und Passwort) in der Regel nicht mehr aus. Erforderlich sind hier Mechanismen der Zwei-Faktor-Authentisierung unter Nutzung eines Hardware-Tokens (Wissen und Besitz), bspw. PIN und Karte wie bei der eID-Funktion des Personalausweises.

Der gesamte Vorgang des Berichtigens MUSS im Bereich des hohen Schutzbedarfs von einem auf die jeweilige Verarbeitungstätigkeit zugeschnittenen standardisierten Prozess gesteuert werden, der die einzelnen Berichtigungsschritte detailliert beschreibt und so zu vollständig standardisierten Abläufen führt (M61.P03).

Werden im Zusammenhang mit der Berichtigung von Daten, deren Verarbeitung zu einem hohen Risiko führt, diese Daten übermittelt, muss auf sichere Übertragungsverfahren zurückgegriffen werden, bspw. Ende-zu-Ende-Verschlüsselung nach dem Stand der Technik oder auch Einschreiben mit Rückschein bei Briefpost (M61.S11).

## 4. Referenzen

*BDSG: http://www.bfdi.bund.de/DE/Datenschutz/Ueberblick/MeineRechte/Artikel/BerichtigungLöschungSperrung.html*

## 5. Zusammenfassung der Maßnahmen

Die einzelnen Maßnahmen können hinsichtlich des Anwendungsbereichs unterschieden werden nach Maßnahmen, welche primär auf einzelne Verarbeitungstätigkeiten angewandt werden sollten (kursive Darstellung) und solche, welche primär die gesamte Organisation

betreffen und damit im Rahmen des Datenschutzmanagements gebündelt und verwaltet werden sollten. Weiterhin sind alle Maßnahmen grob den Phasen des Datenschutzmanagement-Prozesses (siehe SDM-Methode) zugeordnet. Maßnahmen, die in früheren Versionen des Bausteins enthalten waren, aber in einer nachfolgenden Version ungültig wurden, werden weiterhin aufgeführt (durchgestrichene Darstellung). Damit bleibt die Nummer einer Maßnahme bei einer neuen Version erhalten. Die Spalte „Gültigkeit“ gibt an, seit welcher Version die Maßnahme in der enthaltenen Form gültig ist. Bei ungültigen Maßnahmen enthält diese Spalte die Versionsnummer des Bausteins, in der die Maßnahme letztmalig gefordert bzw. empfohlen wurde.

Ebene Daten

| Nr. | Maßnahme | PDCA | Gültigkeit |
|---|---|---|---|
| M61.D01 | *Datenmodell mit geeigneten Datenstrukturen* | P | V1.0 |
| M61.D02 | Kontrolle der Richtigkeit von Daten bei der Rücksicherung und ggf. erneute Berichtigung | D, C | V1.0 |
| M61.D03 | *Datenfelder zur Speicherung von Zeitverläufen und Datenchronologien* | P, C | V1.0 |
| M61.D04 | *Datenfelder zur Speicherung von Zeitangaben oder Zeitstempeln* | P, C | V1.0 |
| M61.D05 | *Datenfelder zur Speicherung identifizierender Daten der Antrag stellenden Person* | P, D, C | V1.0 |
| M61.D06 | *feingranulare, auf einzelne Datenfelder bezogene Berichtigungsmöglichkeit* | P | V1.0 |

Ebene Systeme

| | | | |
|---|---|---|---|
| M61.S01 | Systeme, die Berichtigungsvorgänge zulassen | P, D | V1.0 |
| M61.S02 | Verfahren zur Einschränkung der Verarbeitung von Daten bei Zweifelsfällen | D | V1.0 |
| M61.S03 | *Trennung von Datenbeständen, um differenziert berichtigen zu können* | D | V1.0 |
| M61.S04 | technische Umsetzung des Rechte- und Rollenkonzeptes | P, D | V1.0 |
| M61.S05 | System zur Fristenüberwachung (ggf. im Zusammenhang mit TTS) | D, C | V1.0 |
| M61.S06 | elektronische Zeitstempelsysteme | D, C | V1.0 |
| M61.S07 | Identifizierungssysteme, die Antragsteller sicher identifizieren können | D, C | V1.0 |
| M61.S08 | Identifizierung mit Hilfe der eID-Funktion des neuen Personalausweises | D, C | V1.0 |
| M61.S09 | Protokollierungssysteme | D, C | V1.0 |
| M61.S10 | *Systeme zur Prüfung der Richtigkeit von Daten nach einer Rücksicherung* | D, C | V1.0 |

| | | | |
|---|---|---|---|
| M61.S11 | sichere Übertragungsverfahren wie Ende-zu-Ende-Verschlüsselung nach dem Stand der Technik oder Einschreiben mit Rückschein bei Briefpost | P, D | V1.0 |
| M61. S12 | etablierter Kommunikationskanal mit aktiver Zwei-Faktor-Authentifizierung | P, D | V1.0 |

Ebene Prozesse

| | | | |
|---|---|---|---|
| M61.P01 | Berichtigungskonzept | P | V1.0 |
| M61.P02 | Prozess zur Umsetzung des Rechts betroffener Personen auf Auskunft | P | V1.0 |
| M61.P03 | standardisierter Prozess zur Steuerung des Berichtigungsvorgangs | P | V1.0 |
| M61.P04 | *Dokumentation aller Berichtigungsvorgänge* | D | V1.0 |
| M61.P05 | Festlegung der Pflichten im Zusammenhang mit Berichtigungen zwischen gemeinsamen Verantwortlichen | P | V1.0 |
| M61.P06 | Festlegung der Mitwirkungspflichten von Auftragsverarbeitern | P | V1.0 |
| M61.P07 | Führen eines Verzeichnisses aller Kopien von personenbezogenen Daten | D, C | V1.0 |
| M61.P08 | Möglichkeit der rollenabhängigen Konfigurierung von Berichtigungsprozessen und –rechten | P | V1.0 |
| M61.P09 | Dokumentation von Offenlegungen gegenüber Dritten | D | V1.0 |
| M61.P10 | Prozess zur Fristenüberwachung | D, C | V1.0 |
| M61.P11 | Bereitstellung von Formularen zur Beantragung von Berichtigungen | P | V1.0 |
| M61.P12 | Entgegennahme von Anträge unabhängig von ihrer Form | P, D | V1.0 |
| M61.P13 | Möglichkeiten der elektronischen Beantragung von Berichtigungen | P | V1.0 |
| M61.P14 | Prozess zur Identitätsprüfung von Antragstellern | D, C | V1.0 |
| M61.P15 | Sicherstellung der unverzüglichen Bearbeitung von Anträgen, spätestens innerhalb gesetzlicher Fristen | D, C | V1.0 |
| M61.P16 | Verfahren zur Organisation der Mitteilungspflichten | P, D | V1.0 |
| M61.P17 | Regelungen zur Umsetzung von Berichtspflichten gegenüber Empfängern von zu berichtigenden Daten | P, D | V1.0 |
| M61.P18 | Regelungen zur Umsetzung von Berichtspflichten gegenüber Absendern von nachträglich berichtigten Daten | P, D | V1.0 |
| M61.P19 | Prozess zur ordnungsgemäßen Ablehnung von Berichtigungsanträgen | P, D | V1.0 |
| M61.P20 | *Prozess für turnusmäßige Berichtigungen „im Block“* | D | V1.0 |
| M61.P21 | *Prozess, um den Unterlagen des zuständigen Archivs ggf. eine Gegendarstellung der betroffenen Person hinzuzufügen* | P, D, C | V1.0 |

| | | | |
|---|---|---|---|
| M61.P22 | *Prozess für außerplanmäßige „Korrekturläufe“ von Datensicherungen* | D | V1.0 |
| M61.P23 | *beglaubigte Unterschrift oder beglaubigte Kopie des Personalausweises einfordern* | D | V1.0 |

## 6. Bezug zum Datenschutzmanagement

Dieser Baustein bezieht sich in weiten Teilen auf Anforderungen des Berichtigens von Daten in der gesamten Organisation und bildet die entsprechenden Pflichten des Verantwortlichen ab, welche auf ein einzelnes Verfahren aber auch die gesamte Organisation angewendet werden können. Wird der Baustein auf die die gesamte Organisation angewendet, sind die getroffenen Maßnahmen im Datenschutzmanagement der Organisation zu betrachten.

## 7. Anmerkung zur Nutzung dieses Bausteins

Dieser Baustein darf – ohne Rückfrage bei einer Aufsichtsbehörde – kommerziell und nicht kommerziell genutzt, insbesondere vervielfältigt, ausgedruckt, präsentiert, verändert, bearbeitet sowie an Dritte übermittelt oder auch mit eigenen Daten und Daten Anderer zusammengeführt und zu selbständigen neuen Datensätzen verbunden werden, wenn der folgende Quellenvermerk angebracht wird:

*„Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz). Veränderungen, Bearbeitungen, neue Gestaltungen oder sonstige Abwandlungen der bereitgestellten Daten sind mit einem Veränderungshinweis im Quellenvermerk zu versehen. Datenlizenz Deutschland – Namensnennung – Baustein „Berichtigen“ (www.govdata.de/dl-de/by-2-0).“*