



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Erläuternder Bericht zur Änderung des Bundesgesetzes über die militärischen Informationssysteme

vom 20. Mai 2020

Übersicht

Das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) betreibt diverse, insbesondere militärische Informationssysteme, in denen Personendaten bearbeitet werden. Die vorliegende Änderung des Bundesgesetzes vom 3. Oktober 2008 über die militärischen Informationssysteme (MIG) schafft die datenschutzrechtlich erforderlichen Rechtsgrundlagen, um auch künftig über die für die Aufgabenerfüllung nötigen Personendaten verfügen zu können.

Ausgangslage

Die Bedürfnisse des VBS im Zusammenhang mit der für eine optimale Aufgabenerfüllung notwendigen Bearbeitung von Personendaten in seinen Informationssystemen haben sich – insbesondere auch wegen der erfolgten «Weiterentwicklung der Armee» (WEA) – verändert. Um Personendaten entsprechend dieser neuen Bedürfnisse rechtmässig bearbeiten zu dürfen, setzt das Datenschutzrecht das Bestehen einer gesetzlichen Grundlage voraus. Diese datenschutzrechtlich notwendigen gesetzlichen Grundlagen enthält das MIG aktuell noch nicht. Es sind daher die Bestimmungen des MIG zu den bestehenden Informationssystemen wo nötig anzupassen und Bestimmungen für neue, benötigte Informationssysteme zu schaffen.

Inhalt der Vorlage

Die Vorlage sieht vor, nebst den allgemeinen Bestimmungen des MIG auch die Bestimmungen für bestehende, im MIG geregelte Informationssysteme anzupassen oder Bestimmungen für neue Informationssysteme in das MIG aufzunehmen. Diese Änderungen betreffen insbesondere (a.) die Bearbeitung von neuen Personendaten oder zu neuen Bearbeitungszwecken, (b.) die Beschaffung oder Bekanntgabe von Personendaten bei weiteren beziehungsweise an weitere Stellen, Personen und Informationssysteme, (c.) die Zusammenlegung bestehender Informationssysteme, (d.) die Neuregelung der für die Informationssysteme verantwortlichen Organe, (e.) die Umbenennung von Informationssystemen, (f.) die erleichterte Datenübermittlung mittels Abrufverfahren, Schnittstellen und elektronischer Portale sowie (g.) die Neuregelung der Dauer der Datenaufbewahrung.

Inhaltsverzeichnis

Übersicht	2
1 Ausgangslage	4
1.1 Handlungsbedarf und Ziele	4
1.2 Lösungsvorschlag	4
1.3 Verhältnis zur Legislaturplanung und zu Strategien des Bundesrates	5
1.4 Umsetzungsfragen	5
1.5 Erledigung parlamentarischer Vorstösse	5
2 Grundzüge der Vorlage	5
3 Erläuterung der einzelnen Bestimmungen	7
4 Auswirkungen	26
4.1 Finanzielle, personelle und andere Auswirkungen auf den Bund	26
4.2 Weitere Auswirkungen	26
5 Rechtliche Aspekte	27
5.1 Verfassungsmässigkeit	27
5.2 Vereinbarkeit mit internationalen Verpflichtungen der Schweiz	27
5.3 Erlassform	27
5.4 Unterstellung unter die Ausgabenbremse	27
5.5 Einhaltung des Subsidiaritätsprinzips und des Prinzips der fiskalischen Äquivalenz	27
5.6 Einhaltung der Grundsätze der Subventionsgesetzgebung	28
5.7 Delegation von Rechtsetzungsbefugnissen	28
5.8 Datenschutz	28

Erläuternder Bericht

1 Ausgangslage

1.1 Handlungsbedarf und Ziele

Die Gruppe Verteidigung und die ihr unterstellten Verwaltungseinheiten sind Inhaberinnen und Betreiberinnen diverser militärischer Informationssysteme. Die Bearbeitung von besonders schützenswerten Personendaten und von Persönlichkeitsprofilen in diesen Informationssystemen wird im Bundesgesetz vom 3. Oktober 2008¹ über die militärischen Informationssysteme (MIG) geregelt. Darüber hinaus enthält das MIG auch Bestimmungen zu einzelnen weiteren, innerhalb des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS), jedoch nicht von der Gruppe Verteidigung betriebenen Informationssystemen und der in diesen erfolgenden Personendatenbearbeitung.

Mit der «Weiterentwicklung der Armee» (WEA) wurden die Strukturen, die Organisation und die Prozesse innerhalb der Armee und der Gruppe Verteidigung (sowie der dieser unterstellten Verwaltungseinheiten) grundlegend angepasst. Dabei hat sich auch die Bedürfnislage im Zusammenhang mit der für die Aufgabenerfüllung notwendigen Bearbeitung von Personendaten (insbesondere auch besonders schützenswerten) in Informationssystemen der Gruppe Verteidigung und der ihr unterstellten Verwaltungseinheiten verändert: Bestehende Bedürfnisse bestehen teilweise nicht mehr oder in anderer Weise, und es sind neue Bedürfnisse hinzugekommen. Dasselbe gilt auch mit Bezug auf die ausserhalb der Gruppe Verteidigung betriebenen Informationssysteme des VBS.

Den veränderten oder neuen Bedürfnissen an die Bearbeitung von Personendaten (nachfolgend teilweise auch nur: «Daten») in Informationssystemen des VBS trägt das MIG aktuell nicht Rechnung. Somit fehlen derzeit die datenschutzrechtlich (vgl. Artikel 17 des Bundesgesetzes vom 19. Juni 1992² über den Datenschutz [DSG]) erforderlichen Rechtsgrundlagen, um künftig die Aufgabenerfüllung innerhalb des VBS, insbesondere in der Armee und der Gruppe Verteidigung, umfassend gewährleisten zu können. Es bedarf folglich einer Revision des MIG.

1.2 Lösungsvorschlag

Um den veränderten Bedürfnissen im VBS sowie den datenschutzrechtlichen Anforderungen an die Bearbeitung von Personendaten in Informationssystemen gerecht zu werden, sollen die Bestimmungen des MIG zu den bestehenden Informationssystemen wo nötig angepasst und Bestimmungen für neue, benötigte Informationssysteme, mit denen auch besonders schützenswerte Personendaten und Persönlichkeitsprofile bearbeitet werden sollen, geschaffen werden.

¹ SR 510.91

² SR 235.1

1.3 Verhältnis zur Legislaturplanung und zu Strategien des Bundesrates

Die Anpassungen der im MIG enthaltenen Rechtsgrundlagen zu den militärischen und anderen Informationssystemen des VBS werden im Bundesbeschluss vom 14. Juni 2016³ über die Legislaturplanung 2015–2019 und in der Botschaft vom 29. Januar 2020⁴ zur Legislaturplanung 2019–2023 nicht explizit erwähnt. Da diese Anpassungen jedoch Voraussetzung für eine optimale Erfüllung der dem VBS und insbesondere der Gruppe Verteidigung und der Armee zukommenden gesetzlichen Aufgaben sind, unterstützten sie die Verfolgung von im Bundesbeschluss über die Legislaturplanung 2015–2019 sowie in der Botschaft zur Legislaturplanung 2019–2023 genannten anderen Zielen (etwa das Ziel: «Die Schweiz kennt die [inneren und äusseren] Bedrohungen ihrer Sicherheit und verfügt über die notwendigen Instrumente, um diesen wirksam entgegenzutreten»⁵) und Massnahmen. Weiter tragen die vorgeschlagenen Änderungen und die dadurch erfolgende Optimierung der Informationssystem-Landschaft auch bei zur Erreichung des vom Bundesrat für das Jahr 2020 gesetzten Ziels, staatliche Leistungen effizient und möglichst digital zu erbringen (vgl. Ziele des Bundesrates 2020, Band 1, Ziel 2, S. 12 ff.; siehe auch Botschaft zur Legislaturplanung 2019–2023, Ziel 2⁶).

1.4 Umsetzungsfragen

Die Umsetzung der vorgeschlagenen Lösung soll – unter Vorbehalt der Zustimmung der eidgenössischen Räte zu den beantragten Änderungen der Rechtsgrundlagen – auf den 1. August 2022 erfolgen.

Der vorliegende Erlassentwurf ist durch Ausführungsbestimmungen auf Verordnungsstufe zu konkretisieren. Die inhaltlichen Stossrichtungen ergeben sich aus dem vorliegenden Bericht. Der Bundesrat und das VBS werden diese Ausführungsbestimmungen im Hinblick auf das geplante Inkrafttreten des Erlasses auf den 1. August 2022 rechtzeitig im Voraus erarbeiten und auf denselben Zeitpunkt hin verabschieden.

1.5 Erledigung parlamentarischer Vorstösse

Es werden keine noch offenen parlamentarischen Vorstösse erledigt.

2 Grundzüge der Vorlage

Die Vorlage sieht vor, die Bestimmungen mehrerer bestehender, im MIG geregelter Informationssysteme anzupassen oder Bestimmungen zu neuen Informationssystemen in das MIG aufzunehmen. Diese Änderungen betreffen insbesondere folgende Regelungsgegenstände und Informationssysteme:

³ BBl 2016 5183

⁴ BBl 2020 1777

⁵ BBl 2016 5183, 5190 (Bundesbeschluss über die Legislaturplanung 2015–2019, Ziel 16);

BBl 2020 1777, 1859 f. und 1912 (Botschaft zur Legislaturplanung 2019–2023, Ziel 15)

⁶ BBl 2020 1777, 1835 ff. und 1908

-
- die Ausdehnung des Gegenstands und Geltungsbereichs des MIG unter anderem auch auf Informationssysteme des VBS, einschliesslich der entsprechenden Änderung des Erlassstitels sowie weiteren, dadurch notwendig werdenden Änderungen in anderen Bestimmungen;
 - die Schaffung einer Rechtsgrundlage für die Verwendung und Bearbeitung der AHV-Versichertennummer in nicht militärischen Informationssystemen des VBS;
 - die Integration der in den Ausführungsbestimmungen zum MIG geregelten Informationssysteme in den Verbund der Informationssysteme;
 - die Bekanntgabe von Personendaten an externe, für Wartungs-, Unterhalts- und Programmieraufgaben beigezogene IKT (Informations- und Kommunikationstechnik)-Leistungserbringer;
 - die Integration des Informationssystems Rekrutierung (ITR) und der Falldokumentationsdatenbank des Psychologisch-pädagogischen Dienstes der Armee (FallDok PPD) in das Personalinformationssystem der Armee und des Zivilschutzes (PISA);
 - die Schaffung einer Rechtsgrundlage für die Bearbeitung weiterer Personendaten in diversen Informationssystemen (PISA, Informationssystem Evaluation Armee-Auklärungsdetachment [EAAD], Informationssystem Militärische Fahrberechtigungen [MIFA]);
 - die Präzisierung der Rechtsgrundlage für die Bearbeitung von Personendaten im Informationssystem Schadenzentrum VBS (SCHAWA);
 - die Schaffung einer Rechtsgrundlage, damit die in den Informationssystemen oder beim Einsatz von Überwachungsmitteln bearbeiteten Personendaten bei weiteren Stellen, Personen oder Informationssystemen beschafft bzw. an diese bekannt gegeben oder zu neuen Zwecken bearbeitet werden dürfen;
 - die Nennung der Gruppe Verteidigung als Betreiberin diverser Informationssysteme (PISA, Informationssysteme Patientenerfassung [ISPE], Informationssystem Flugmedizin [MEDIS LW], Informationssystem Sozialer Bereich [ISB], Informations- und Einsatz-System Koordinierter Sanitätsdienst [IES-KSD]), wodurch die untergeordneten Verwaltungseinheiten, die Inhaberinnen der Datensammlungen und für den Datenschutz verantwortliche Bundesorgane sind, in den Ausführungsbestimmungen auf Verordnungsstufe definiert werden können;
 - die Umbenennung von Informationssystemen (EAAD, ISB, MIFA, Journal- und Rapportsystem der Militärischen Sicherheit [JORASYS], SCHAWA, Strategisches Informationssystem Logistik [SISLOG]);
 - die Schaffung einer Rechtsgrundlage für die Verwendung gewisser Daten des Informationssystems Administration für Dienstleistungen (MIL Office) zur Verhinderung von Missbräuchen der Erwerbersatzordnung und für deren Bekanntgabe an die Zentrale Ausgleichsstelle;
 - die Regelung des Betriebs eines elektronischen Portals für die freiwillige elektronische Übermittlung der im MIL Office bearbeiteten Personendaten (z. B. Urlaubsgesuche mit Beilagen) an die zuständigen militärischen Kommandos;

-
- die Verlängerung (Informationssysteme von Simulatoren, Informationssystem Ausbildungsmanagement [Learning Management System, LMS VBS], MIFA) bzw. Neuregelung (MEDIS LW, JORASYS) der Aufbewahrungsdauer von Personendaten;
 - die Ermöglichung des durch Abrufverfahren oder automatisiert über eine Schnittstelle erfolgenden Datenzugriffs (Informationssystem Personensicherheitsprüfung [SIBAD], JORASYS);
 - die Neu-Aufnahme einer Regelung für das Informationssystem Präventiver Schutz der Armee (IPSA; dient dem Dienst für präventiven Schutz der Armee [DPSA] zur Aufgabenerfüllung sowie zur Journal- und Einsatzführung) und für das Informationssystem Master-Data-Management (MDM; bezweckt die Verwaltung und Bereitstellung einheitlicher und eindeutiger Stammdaten von Geschäftspartnerinnen und Geschäftspartnern für diverse Geschäftsprozesse im VBS);
 - rein formelle, rechtsetzungstechnisch bedingte oder sprachliche Änderungen (allgemeine Bestimmungen, PISA, Medizinisches Informationssystem der Armee [MEDISA], Informationssystem Personal Verteidigung [IPV], IES-KSD, MIL Office, Informationssystem Kompetenzmanagement [ISKM], Führungsinformationssystem Soldat [IMESS], MIFA, JORASYS, Informationssystem integrierte Ressourcenbewirtschaftung [PSN]).

3 Erläuterung der einzelnen Bestimmungen

Erlasstitel

Das MIG regelt bereits heute auch die Bearbeitung von Personendaten in diversen Informationssystemen, die nicht von der Gruppe Verteidigung, sondern von anderen Verwaltungseinheiten innerhalb des VBS betrieben werden. Der auf militärische Informationssysteme beschränkte Erlasstitel ist dementsprechend zu erweitern, wobei jedoch die gängige Abkürzung MIG beibehalten werden soll.

Ingress

Zusätzlich zu den im Ingress bereits genannten Bestimmungen (Artikel 40 Absatz 2 und Artikel 60 Absatz 1 der Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999⁷ [BV]), welche die Rechtsgrundlage für die Regelung der militärischen Informationssysteme bilden, ist als weitere Rechtsgrundlage für die im MIG geregelten «anderen», nicht militärischen Informationssysteme des VBS (mangels Vorhandensein einer expliziten Kompetenznorm zugunsten des Bundes) praxisgemäss der Artikel 173 Absatz 2 BV zu ergänzen.

Art. 1 Abs. 1 Einleitungssatz und Bst. b, c und d sowie Abs. 2

Der zu eng gefasste Geltungsbereich ist derart zu erweitern, dass nicht nur die militärischen Informationssysteme, sondern auch die bereits heute im MIG geregelten «anderen», nicht militärischen Informationssysteme, die das VBS betreibt, erfasst werden (vgl. Artikel 1 Absatz 1 Einleitungssatz). Da die Personendaten in diesen nicht militärischen Informationssystemen des VBS nicht nur bearbeitet werden, um Aufgaben im Zusammenhang mit dem Militärwesen zu erfüllen, sondern auch für das VBS, bedarf es einer entsprechenden Ergänzung in Artikel 1 Absatz 1 Buchstabe d. Weiter werden in diversen, im MIG geregelten Informationssystemen Personendaten im Zusammenhang mit dem Zivilschutz bearbeitet, weshalb in Artikel 1 Absatz 1 Buchstaben b, c und d auch die entsprechenden Personen des Zivilschutzes bzw. Dritte, die Aufgaben für das Zivilschutzwesen erfüllen, zu nennen sind. Artikel 1 Absatz 1 Buchstabe b ist überdies geschlechtergerecht zu formulieren.

Weiter wird im Einleitungssatz von Artikel 1 Absatz 1 durch die zusätzliche Erwähnung von «anderen» Personendaten (nebst den besonders schützenswerten Personendaten und den Persönlichkeitsprofilen) der Tatsache Rechnung getragen, dass die im MIG enthaltenen Bestimmungen zu den einzelnen Informationssystemen nicht nur die Bearbeitung von besonders schützenswerten Personendaten (im Sinn von Artikel 3 Buchstabe c DSGVO) und Persönlichkeitsprofilen (im Sinn von Artikel 3 Buchstabe d DSGVO) vorsehen, sondern explizit auch von anderen, nicht besonders schützenswerten Personendaten (wie etwa Personalien, vgl. so z. B. geregelt in den Artikeln 128 Buchstabe b, 143c Buchstabe a, 167c Absatz 1 Buchstabe a, 179c Absatz 1 Buchstabe a und 179i Buchstabe a MIG).

Der Artikel 1 Absatz 2 ist dahingehend zu präzisieren, dass lediglich die (andernorts geregelte) Datenbearbeitung durch den Nachrichtendienst vom Geltungsbereich ausgenommen ist, jedoch nicht gänzlich jede Bearbeitung von Daten, die den Nachrichtendienst bzw. etwa dessen Mitarbeiterinnen und Mitarbeiter betreffen.

Art. 2 Abs. 1 Einleitungssatz und Bst. a

Aufgrund des zu erweiternden, auch nicht militärische Informationssysteme des VBS umfassenden Geltungsbereichs des MIG (vgl. Erläuterungen zu Artikel 1 Absatz 1 Einleitungssatz) gelten dessen allgemeinen Bestimmungen, insbesondere Artikel 2 (Grundsätze der Datenbearbeitung), gleichermaßen für diese nicht militärischen Informationssysteme des VBS. Dies wird mit der vorgesehenen Erweiterung im Einleitungssatz von Artikel 2 Absatz 1 verdeutlicht. Mit dieser Erweiterung wird insbesondere auch die nach Artikel 50e Absatz 1 des Bundesgesetzes vom 20. Dezember 1946⁸ über die Alters- und Hinterlassenenversicherung erforderliche rechtliche Grundlage für die Verwendung der AHV-Versichertennummer in nicht militärischen Informationssystemen des VBS geschaffen. Da im Rahmen der Erfüllung der gesetzlichen Aufgaben zahlreiche Berührungspunkte zwischen den Verwaltungseinheiten des VBS, die nicht zur Gruppe Verteidigung gehören, einerseits sowie der Armee und Militärverwaltung andererseits bestehen und entsprechend diverse Informationssysteme (z. B. LMS VBS, Identitätsverwaltungs-System [ICAM]) über-

greifend für das gesamte VBS betrieben werden, ist die Verwendung der AHV-Versichertennummer als Personenidentifikator auch im nicht militärischen Bereich des VBS für eine optimale, effiziente Verwaltungstätigkeit und Aufgabenerfüllung unerlässlich.

Artikel 2 Absatz 1 Buchstabe a ist aufzuheben, da sich einerseits das darin geregelte Erfordernis einer rechtlichen Grundlage für die Bearbeitung von Personendaten und für das Zugänglichmachen mittels Abrufverfahren bereits aus den (gemäss Artikel 1 Absatz 3 MIG auch hier anwendbaren) Artikeln 17 und 19 Absatz 3 DSG ergibt. Andererseits ist die Regelung in Artikel 2 Buchstabe a auf den derzeit bestehenden Artikel 1 Absatz 1 MIG gemünzt und trifft für die in Artikel 1 Absatz 1 neu (vgl. die vorstehenden Erläuterungen) zu erwähnende Bearbeitung von Personendaten, die nicht besonders schützenswert und auch nicht als Persönlichkeitsprofil zu qualifizieren sind, nicht mehr zu. Für die Bearbeitung von solchen, nicht besonders schützenswerten Personendaten oder deren Zugänglichmachen mittels Abrufverfahren bedarf es keiner rechtlichen Grundlage in einem Gesetz im formellen Sinn, es genügt vielmehr eine Bestimmung in einer Verordnung des Bundesrates (vgl. Artikel 17 und 19 Absatz 3 DSG, Artikel 186 Absatz 1 Buchstabe b MIG).

Art. 3

Aufgrund des zu erweiternden, auch nicht militärische Informationssysteme des VBS umfassenden Geltungsbereichs des MIG (vgl. Erläuterungen zu Artikel 1 Absatz 1 Einleitungssatz) sind insbesondere für die nicht militärischen Informationssysteme auch weitere Leistungserbringer neben der Führungsunterstützungsbasis der Armee denkbar. Artikel 3 ist daher aufzuheben. Der technische Betreiber eines jeweiligen Informationssystems kann etwa im Bearbeitungsreglement (vgl. Artikel 36 Absatz 4 DSG i.V.m. Artikel 21 der Verordnung vom 14. Juni 1993⁹ zum Bundesgesetz über den Datenschutz) festgelegt werden.

Art. 4 Abs. 1

Aufgrund des zu erweiternden, auch nicht militärische Informationssysteme des VBS umfassenden Geltungsbereichs des MIG (vgl. Erläuterungen zu Artikel 1 Absatz 1 Einleitungssatz) sollen mit der Abänderung des Artikel 4 Absatz 1 auch die nicht militärischen Informationssysteme des VBS in den in Artikel 4 geregelten Verbund von Informationssystemen eingebunden werden können. Ausserdem soll die in den Ausführungsbestimmungen zum MIG (vgl. Artikel 2 Absatz 2 der Verordnung vom 16. Dezember 2009¹⁰ über die militärischen Informationssysteme [MIV]) bereits enthaltene Regelung, welche die Einbindung der ausschliesslich in diesen Ausführungsbestimmungen geregelten Informationssysteme in den Verbund gemäss Artikel 4 MIG vorsieht, der Vollständigkeit halber auch auf Gesetzesstufe verankert werden.

⁹ SR 235.11

¹⁰ SR 510.911

Art. 6

Der bisherige Artikel 6 MIG regelt die Anforderungen an die Regelungsstufe (formelles Gesetz oder dem fakultativen Referendum unterstehender Staatsvertrag) der Rechtsgrundlage, die für die Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen (vgl. so der derzeitige Geltungsbereich gemäss Artikel 1 Absatz 1 MIG) im Rahmen der internationalen Zusammenarbeit benötigt wird. Um dieses Erfordernis mit der geplanten Erweiterung des Geltungsbereichs des MIG (vgl. Erläuterungen zu Artikel 1 Absatz 1 Einleitungssatz) nicht auf die (neu auch unter den Geltungsbereich fallenden) nicht besonders schützenswerten Personendaten auszudehnen, ist Artikel 6 entsprechend anzupassen. Für die Bearbeitung von nicht besonders schützenswerten Personendaten im Rahmen der in Artikel 6 geregelten internationalen Zusammenarbeit sollen als Rechtsgrundlage die vom Bundesrat erlassenen Ausführungsbestimmungen zum MIG oder ein vom Bundesrat abgeschlossenes internationales Abkommen ausreichend sein. Diese Regelungsstufe erscheint im Lichte der Artikel 17 Absatz 2 und 19 Absatz 3 DSGVO angebracht, wo jeweils bloss für die Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen eine Regelung in einem formellen Gesetz verlangt wird.

Art. 7 Abs. 2 erster Satz

Bundesinterne IKT (Informations- und Kommunikationstechnik)-Leistungserbringer sind aus Kosten- und Effizienzgründen auf die Zusammenarbeit mit externen IKT-Dienstleistern ausserhalb der eigenen Verwaltungseinheit oder ausserhalb der Bundesverwaltung angewiesen. Dies kann mit sich bringen, dass diesen externen IKT-Dienstleistern in Einzelfällen bei anstehenden Wartungs-, Unterhalts- oder Programmieraufgaben personenbezogene Daten, die nicht allgemein zugänglich sind, offenbart werden müssen, damit der Betrieb der Informationssysteme aufrechterhalten oder zumindest eine allfällige Unterbrechungszeit auf ein absolutes Minimum reduziert werden kann. Daher ist in Artikel 7 Absatz 2 erster Satz der Klarheit halber zu verdeutlichen, dass zu den betrauten Personen, die unter den genannten Voraussetzungen zur Datenbearbeitung berechtigt sind, auch beigezogene (verwaltungseinheits- oder verwaltungs-)externe IKT-Leistungserbringer zählen.

Art. 8

Die bestehende Bestimmung des Artikel 8 soll einfacher und entsprechend dem zeitlich-logischen Ablauf der Datenhaltung und -archivierung formuliert werden. Anders als im bestehenden Artikel 8 soll daher neu die Löschung nicht benötigter Daten nicht mehr vor dem Anbieten zur Archivierung genannt werden (vgl. Artikel 8 zweiter Satz). Zudem ist nur noch der Begriff der «Vernichtung» (im Sinne einer endgültigen, nicht rückgängig machbaren Löschung) der Daten zu verwenden und nicht noch zusätzlich derjenige der «Löschung» der Daten.

Art. 11

Die Fragen, welche Personendaten in einem Informationssystem zu welchem Zweck wie und in welcher Form bearbeitet und wie lange aufbewahrt werden dürfen, sind in den besonderen Bestimmungen zu den einzelnen Informationssystemen zu regeln und dort auch bereits geregelt, weshalb Artikel 11 aufgehoben werden kann.

Art. 13 Bst. n, o und p, 14 Abs. 1 Bst. a^{bis}, c^{bis} und n, Abs. 2 Einleitungssatz und Abs. 4, 15 Abs. 1 Einleitungssatz und Abs. 4, 16 Abs. 1 Einleitungssatz und Bst. b^{bis} sowie Abs. 1^{ter}, 17 Abs. 4^{ter}, 4^{quater} und 5 (Informationssystem PISA)

Die bestehende Regelung des PISA soll an die aktuellen Gegebenheiten und Bedürfnisse angepasst respektive diesen entsprechend erweitert werden.

Die Hauptänderungen betreffen die Integration von zwei bestehenden Informationssystemen – dem ITR (vgl. Artikel 18 ff. MIG) und der FallDok PPD (vgl. Artikel 36 ff. MIG) – in das PISA. Hierzu sind in den PISA-Bestimmungen die nötigen Anpassungen und Erweiterungen wie folgt vorzunehmen:

- Für die Integration des ITR sind die Artikel 14 Absatz 1 Buchstabe a^{bis} (aus dem Artikel 20 Absatz 2 MIG inhaltlich unverändert übernommener Katalog der bearbeiteten Personendaten), 16 Absatz 1 Einleitungssatz und Buchstabe b^{bis} (wie heute in Artikel 22 Absatz 1 MIG für das ITR geregelt, sollen auch künftig die mit der Rekrutierung beauftragten Ärztinnen und Ärzte durch Aburverfahren Zugang zu den für die Aufgabenerfüllung benötigten Daten des PISA, insbesondere diejenigen nach Artikel 14 Absatz 1 Buchstabe a^{bis}, haben) sowie 17 Absatz 4^{ter} (wie bisher im ITR [vgl. Artikel 23 MIG] sind die an der Rekrutierung erhobenen sanitätsdienstlichen Daten [vgl. zum Begriff Artikel 26 Absatz 2 MIG] in das MEDISA zu überführen und innert Wochenfrist seit der Datenerhebung im PISA wieder zu löschen) anzupassen. Die übrigen ITR-Bestimmungen sind in den PISA-Bestimmungen inhaltlich bereits abgedeckt.
- Für die Integration der FallDok PPD sind Änderungen in den Artikeln 13 Buchstabe o (Zweck der Datenbearbeitung; entspricht Artikel 37 Buchstabe a MIG), 14 Absatz 4 (bearbeitete Personendaten; entspricht Artikel 38 MIG), 15 Absatz 4 (Datenbeschaffung; entspricht Artikel 39 MIG), 16 Absatz 1^{ter} (Datenbekanntgabe; entspricht Artikel 40 Absatz 1 MIG – die gemäss dem heutigen Artikel 40 Absatz 2 MIG bekanntzugebenden Daten werden von Artikel 14 Absatz 1 MIG erfasst und können daher gemäss Artikel 15 Absatz 1 Buchstabe d MIG beim Psychologisch-pädagogischen Dienst der Armee [PPD] beschaffen und gestützt auf Artikel 16 Absatz 1 Buchstaben a und b MIG den Militärbehörden und militärischen Kommandos bekannt gegeben werden) und 17 Absatz 4^{quater} (Datenaufbewahrung; entspricht Artikel 41 MIG) erforderlich.

Weiter ist mit der vorgesehenen Ergänzung am Ende des Einleitungssatzes des Artikels 16 Absatz 1 die Datenbekanntgabe im Sinne des Verhältnismässigkeitsgrundsatzes bei der Datenbearbeitung (vgl. Artikel 4 Absatz 2 DSG) – auch angesichts der erfolgenden Integration etwa des ITR und der FallDok PPD sowie der

damit unter anderem ins PISA fließenden sanitätsdienstlichen Daten – derart einzuschränken, als dass die Bekanntgabe der PISA-Daten durch Abrufverfahren nur erfolgen soll, soweit dies zur Erfüllung von gesetzlichen oder vertraglichen Aufgaben notwendig ist. Entsprechend ist durch Zugriffsbeschränkungen sicherzustellen, dass nicht alle Stellen und Personen sämtliche Daten (wie etwa sanitätsdienstliche Rekrutierungsdaten gemäss Artikel 14 Absatz 1 Buchstabe a^{bis}), sondern nur die von ihnen tatsächlich Benötigten sehen können.

Die Änderungen in den Artikeln 13 Buchstabe n und 14 Absatz 1 Buchstabe n sollen die Bearbeitung der PISA-Daten im Zusammenhang mit der Prüfung und der Kontrolle von Ausbildungsgutschriften ermöglichen. Die PISA-Daten sollen zudem gemäss dem neuen Artikel 13 Buchstabe p auch für die anonymisierte Beantwortung gestellter Anfragen zu statistischem Zahlenmaterial betreffend das VBS beigezogen werden dürfen. Überdies sollen auch Daten über absolvierte Ausbildungen und erlangte Berechtigungen von militärischen Systemen im PISA erfasst werden (vgl. Artikel 14 Absatz 1 Buchstabe c^{bis}), um etwa die personellen Bestände der Armee optimal zuteilen, planen und bewirtschaften zu können. Mit der Änderung in Artikel 17 Absatz 5 bzw. mit dem neu hinzukommenden Wort «längstens» soll klargestellt werden, dass eine Löschung der übrigen, nicht von den vorangehenden Absätzen des Artikels 17 MIG erfassten PISA-Daten auch schon vor Ablauf von fünf Jahren (z. B. jahrgangswise Löschung) möglich ist und eine fünfjährige Aufbewahrungsdauer nicht zwingend erforderlich ist.

Die Änderung in Artikel 14 Absatz 2 ist untergeordneter, rein sprachlicher bzw. rechtsetzungstechnischer Natur. Der Bezug zum PISA ergibt sich bereits aus Artikel 14 Absatz 1 MIG, weshalb eine Wiederholung der Abkürzung des Informationssystems in Artikel 14 Absatz 2 unnötig ist. Eine weitere Änderung betrifft den Einleitungssatz von Artikel 15 Absatz 1, der geschlechtergerecht formuliert werden soll.

Art. 18–23 (Informationssystem ITR)

Mit der Integration des ITR in das PISA und der neu im PISA erfolgenden Bearbeitung der ITR-Daten (vgl. Artikel 14 Absatz 1 Buchstabe a^{bis}) können die bestehenden Bestimmungen zum ITR aufgehoben werden.

Art. 24, 27 Einleitungssatz, 28 Abs. 1 Einleitungssatz und Bst. c sowie Abs. 3 Einleitungssatz (Informationssystem MEDISA)

Wie auch bei den anderen, im MIG geregelten Informationssystemen der Gruppe Verteidigung üblich, soll als Betreiberin des MEDISA nur noch die Gruppe Verteidigung (als übergeordnete Verwaltungseinheit i.S.v. Anhang 1 der Regierungs- und Verwaltungsorganisationsverordnung vom 25. November 1998¹¹ [RVOV]) erwähnt werden (in Artikel 24 sowie in den Einleitungssätzen der Artikel 27 sowie 28 Absätze 1 und 3). Die untergeordnete Verwaltungseinheit, die Inhaberin der Datensammlung und für den Datenschutz verantwortliches Bundesorgan ist, ist in den Ausführ-

¹¹ SR 172.010.1

rungsbestimmungen auf Verordnungsstufe zu definieren (vgl. Artikel 2a und Anhang 1 MIV).

Die Änderung des Artikels 28 Absatz 1 Buchstabe c ist bloss formeller Art und rechtsetzungstechnisch bedingt (Verwendung der neu bereits zuvor in Artikel 14 Absatz 4 eingeführten Abkürzung «PPD»).

Art. 30 und 33 Einleitungssatz (Informationssysteme ISPE)

Wie auch bei den anderen, im MIG geregelten Informationssystemen der Gruppe Verteidigung üblich, soll als Betreiberin der ISPE nur noch die Gruppe Verteidigung (als übergeordnete Verwaltungseinheit i.S.v. Anhang 1 RVOV) erwähnt werden. Die untergeordnete Verwaltungseinheit, die Inhaberin der Datensammlung und für den Datenschutz verantwortliches Bundesorgan ist, ist in den Ausführungsbestimmungen auf Verordnungsstufe zu definieren (vgl. Artikel 2a und Anhang 1 MIV).

Art. 36–41 (Informationssystem FallDok PPD)

Mit der Integration der FallDok PPD in das PISA und der neu im PISA erfolgenden Bearbeitung der FallDok PPD-Daten (vgl. Artikel 14 Absatz 4) können die bestehenden Bestimmungen zum ITR aufgehoben werden.

Art. 42, 45 Einleitungssatz, 46 Abs. 1 Einleitungssatz und Abs. 2 sowie 47 Abs. 1 und 3 (Informationssystem MEDIS LW)

Wie auch bei den anderen, im MIG geregelten Informationssystemen der Gruppe Verteidigung üblich, soll als Betreiberin des MEDIS LW nur noch die Gruppe Verteidigung (als übergeordnete Verwaltungseinheit i.S.v. Anhang 1 RVOV) erwähnt werden. Die untergeordnete Verwaltungseinheit, die Inhaberin der Datensammlung und für den Datenschutz verantwortliches Bundesorgan ist, ist in den Ausführungsbestimmungen auf Verordnungsstufe zu definieren (vgl. Artikel 2a und Anhang 1 MIV). Artikel 47 Absatz 1 ist aufzuheben, da gemäss Artikel 8 MIG und dem Bundesgesetz vom 26. Juni 1998¹² über die Archivierung (Archivierungsgesetz, BGA) die Archivierung der nicht mehr ständig benötigten Unterlagen durch das Bundesarchiv erfolgt. Die Bearbeitung von Daten des MEDIS LW in nicht elektronischer Form lässt Artikel 2 Absatz 3 MIG weiterhin zu. Mit der neuen Regelung in Artikel 47 Absatz 3 soll zudem sichergestellt werden, dass die Daten von Personen, die sich bei Ablauf der Aufbewahrungsdauer nach dem bestehenden Artikel 47 Absatz 2 MIG weiterhin (z. B. über das vollendete 80. Lebensjahr hinaus) durch das fliegerärztliche Institut behandeln oder betreuen lassen, nach Abschluss der Behandlung oder Betreuung noch während zehn Jahren bearbeitet und aufbewahrt werden können.

Gliederungstitel vor Art. 48, Art. 48, 49 Einleitungssatz sowie Bst. a und b, 50, 51 Einleitungssatz, 52 Abs. 1 und 53 Abs. 2 (Informationssystem EAD)

Nebst den Daten der Angehörigen des zum Kommando Spezialkräfte (KSK) gehörenden Armee-Aufklärungsdetachements sowie des Einsatzunterstützungspersonals (Führung, Logistik, Führungsunterstützung) sollen auch die Daten der zu evaluierenden Anwärterinnen und Anwärter sowie Angehörigen des Militärpolizei-Spezialdetachements, welches ebenfalls Teil des KSK ist, bearbeitet werden. Die Bezeichnung des Informationssystems (mitsamt Abkürzung) sowie einzelne, den betroffenen Personenkreis nennende Bestimmungen (Artikel 49 Buchstaben a und b sowie 53 Absatz 2) sind daher derart auszugestalten, dass sämtliche vorgenannten Personen mit umfasst werden.

Gliederungstitel vor Art. 54, Art. 54–58 (Informationssystem ISB)

Wie auch bei den anderen, im MIG geregelten Informationssystemen der Gruppe Verteidigung üblich, soll als Betreiberin des Informationssystems nur noch die Gruppe Verteidigung (als übergeordnete Verwaltungseinheit i.S.v. Anhang 1 RVOV) erwähnt werden. Die untergeordnete Verwaltungseinheit, die Inhaberin der Datensammlung und für den Datenschutz verantwortliches Bundesorgan ist, ist in den Ausführungsbestimmungen auf Verordnungsstufe zu definieren (vgl. Artikel 2a und Anhang 1 MIV).

Die geplante Änderung des Namens des Informationssystems (neu «Informationssystem für die soziale Beratung» anstatt «Informationssystem Sozialer Bereich») ist im Gliederungstitel vor Artikel 54 sowie in Artikel 54 anzupassen.

Die Zweckbestimmung in Artikel 55 ist dahingehend zu erweitern, dass auch Angehörige des Zivilschutzes und des Rotkreuzdienstes, Personen im Friedensförderungsdienst, Angehörige der Militärjustiz sowie die Angehörigen der in Artikel 55 genannten Personen mit umfasst werden. Denn auch diese werden vom Sozialdienst der Armee gestützt auf die Verordnung vom 30. November 2018¹³ über den Sozialfonds für Verteidigung und Bevölkerungsschutz unterstützt.

Für die Begründung seiner Entscheide für finanzielle Unterstützungen benötigt der Sozialdienst der Armee nebst den in Artikel 56 bereits genannten Angaben zur geleisteten finanziellen Unterstützung auch Angaben zur Fallführung, Notizen zur Gesprächsführung sowie persönliche Unterlagen und Dokumente, die für die Beurteilung einer sozialen Beratung und Betreuung (z. B. auch finanzielle Unterstützung) notwendig sind. Entsprechend sind diese Daten in Artikel 56 zu ergänzen. Als neue Datenbezugsquelle ist zudem in Artikel 57 das PISA zu nennen. Die Datenbeschaffung aus dem PISA dient der Planung von Gesprächen und beschränkt sich auf Personalien und die AHV-Versichertennummer. Zudem muss bei der Auszahlung von Geldern des Sozialfonds für Verteidigung und Bevölkerungsschutz im PISA geprüft werden, ob die Person noch militärdienstpflichtig ist oder ob sie zwischenzeitlich entlassen wurde und damit keinen Anspruch mehr hätte.

¹³ SR 611.021

Weiter sind in Artikel 58 Buchstabe b die beim Fachstab des Sozialdienstes der Armee eingeteilten Armeeeingehörenden, welche ebenfalls zur Erfüllung des unter Artikel 55 MIG genannten Zwecks bzw. der Aufgaben des Sozialdienstes der Armee beitragen und daher Zugang zu den Daten des ISB benötigen, zusätzlich explizit zu nennen; denn diese Armeeeingehörenden sind nicht Mitarbeitende (im Sinne von Arbeitnehmerinnen und Arbeitnehmer) des Sozialdienstes der Armee, sondern Teil der Milizarmee. Ferner sollen mit den in Artikel 58 neu einzufügenden Buchstaben c und d auch die Fachstelle Diversity Schweizer Armee und die Armeeseelsorge, die beide ebenfalls soziale Beratungen für Armeeeingehörende anbieten, durch Abrufverfahren Zugriff jeweils nur auf die ihre eigenen Klientinnen und Klienten betreffenden Daten des ISB erhalten.

Art. 63 Abs. 2 und 65 Abs. 2 (Informationssystem IPV)

Das Personalinformationssystem der Bundesverwaltung (BV PLUS) wurde durch das neu in den Artikeln 30–38 der Verordnung vom 22. November 2017¹⁴ über den Schutz von Personendaten des Bundespersonals (BPDV) geregelte Informationssystem für das Personalmanagement (IPDM) abgelöst. Entsprechend ist in Artikel 63 Absatz 2 das IPDM anstelle des BV PLUS als Datenbezugsquelle zu nennen. In Artikel 65 Absatz 1 ist überdies entsprechend der in Artikel 8 neu verwendeten Begrifflichkeit (vgl. Erläuterungen zu Artikel 8) das Wort «gelöscht» durch «vernichtet» zu ersetzen.

Art. 72 und 73 Einleitungssatz (Informationssystem IES-KSD)

Wie auch bei den anderen, im MIG geregelten Informationssystemen der Gruppe Verteidigung üblich, soll als Betreiberin des IES-KSD nur noch die Gruppe Verteidigung (als übergeordnete Verwaltungseinheit i.S.v. Anhang 1 RVOV) erwähnt werden. Die untergeordnete Verwaltungseinheit, die Inhaberin der Datensammlung und für den Datenschutz verantwortliches Bundesorgan ist, ist in den Ausführungsbestimmungen auf Verordnungsstufe zu definieren (vgl. Artikel 2a und Anhang 1 MIV). Ferner ist die durch die Anpassung in Artikel 72 wegfallende Abkürzung «KSD» neu im Einleitungssatz von Artikel 73 einzuführen.

Art. 85 Abs. 2, 86 Bst. a, a^{bis} und h, 87 Bst. a sowie 88 (Informationssystem MIL Office)

Zur Verhinderung von Missbräuchen der Erwerbssatzordnung soll mit den zu ändernden Artikel 85 Absatz 2 und 88 (neuer Buchstabe d) eine Rechtsgrundlage geschaffen werden, damit die im MIL Office enthaltenen Daten zu Sold- und Spesenabrechnungen sowie zu Absenzen und Kommandierungen zusammen mit weiteren Daten (Personalien, Adresse, Kontaktangaben sowie Daten über Einteilung, Grad, Funktion und Ausbildung) an die Zentrale Ausgleichsstelle bekannt gegeben werden dürfen.

Weiter soll in Artikel 87 Buchstabe a die Rechtsgrundlage für den Betrieb eines elektronischen Portals, über welches Personendaten (wie etwa Urlaubsgesuche mit Beilagen) von der betreffenden Person freiwillig an das für sie zuständige militärische Kommando übermittelt werden können. Durch diese Möglichkeit werden die Abläufe im Zusammenhang mit der Verwaltung und dem Betrieb in Schulen und Kursen (vgl. so der in Artikel 85 MIG genannte Zweck des MIL Office) für alle Beteiligten verkürzt und vereinfacht.

Mit den Anpassungen in Artikel 86 (Neuaufnahme der Buchstaben a und h; bisheriger Buchstabe a wird zu Buchstabe a^{bis}) werden die in den Ausführungsbestimmungen (vgl. Anhang 16 Ziffern 1, 5 und 12 MIV) bereits definierten (nicht besonders schützenswerten) Personendaten, die im MIL Office bearbeitet werden, der Klarheit und Vollständigkeit halber auch im MIG abgebildet.

Art. 94 (Informationssystem ISKM)

Wie in zahlreichen anderen Bestimmungen des MIG, welche die Bekanntgabe von Daten eines Informationssystems regeln, soll der Einheitlichkeit halber auch in Artikel 94 die Bekanntgabe nicht nur an «Personen», sondern an «Stellen und Personen» erwähnt werden.

Art. 103 Einleitungssatz sowie Bst. a und c (Führungsinformationssystem Heer [FIS HE])

Das FIS HE soll einerseits nicht mehr zur Aktionsführung, dafür aber zur Lageverfolgung eingesetzt werden können und andererseits auch dem gesamten Kommando Operationen sowie der Führungsunterstützungsbasis bei der Aufgabenerfüllung dienen. Hierfür ist die Zweckbestimmung in Artikel 103 Buchstaben a und c entsprechend zu erweitern. Die Änderungen im Einleitungssatz sind rein sprachlicher Natur.

Art. 109 Bst. a und 110 Bst. a (Führungsinformationssystem Luftwaffe [FIS LW])

Das FIS LW soll nicht mehr zur Aktionsführung, dafür aber zur Lageverfolgung eingesetzt werden können. Hierfür ist die Zweckbestimmung in Artikel 109 Buchstabe a entsprechend zu erweitern.

Weiter kann in Artikel 110 Buchstabe a die im FIS LW nicht bearbeitete Religionszugehörigkeit gestrichen werden.

Art. 119 (Führungsinformationssystem Soldat [IMESS])

In Artikel 119 ist entsprechend der in Artikel 8 neu verwendeten Begrifflichkeit (vgl. Erläuterungen zu Artikel 8) das Wort «gelöscht» durch «vernichtet» zu ersetzen.

Art. 121, 123 Bst. c, 124 Abs. 2 Bst. c und 125 Abs. 2 (Informationssysteme von Simulatoren)

Die Trainingsdaten von Personen, die regelmässig Trainings an Simulatoren absolvieren, sollen (möglichst) während ihrer gesamten, in der Regel fünf Jahre übersteigenden Verweildauer in der Armee verfügbar sein und aufbewahrt werden können. Entsprechend ist in Artikel 125 Absatz 2 die bisherige fünfjährige Aufbewahrungsdauer auf zehn Jahre zu verlängern. Weiter ist in den einzelnen Bestimmungen (Artikel 121, 123 Buchstabe c, 124 Absatz 2 und 125 Absatz 2) vorzusehen, dass auch die Daten von (nicht für einen befristeten Einsatz der Armee beigezogenen) Zivilpersonen oder Dritten (etwa von Blaulichtorganisationen), die an den Simulatoren trainieren, bearbeitet und bei deren zivilen Vorgesetzten beschaffen bzw. diesen bekannt gegeben werden dürfen.

Art. 131 (Informationssystem LMS VBS)

Angehörige der Armee und Angestellte des VBS nehmen erfahrungsgemäss während zehn Jahren nach ihrer Entlassung aus der Militärdienstpflicht bzw. nach Beendigung ihres Arbeitsverhältnisses beim VBS häufig noch an ausserdienstlichen Tätigkeiten teil oder werden beim Bund weiterbeschäftigt. Um weiterhin Kenntnis über die von Armeeingehörigen oder von Angestellten des VBS im LMS VBS erworbenen, für ausserdienstliche Tätigkeiten oder für eine Weiterbeschäftigung beim Bund erforderlichen Fähigkeiten (z. B. von ausserdienstlich eingesetzten Motorfahrerinnen und -fahrern in den Bereichen Gefahrguttransport oder Ladesicherung oder von eidgenössischen Schiessoffizierinnen und -offizieren im Bereich allgemeiner Sicherheitsvorschriften) zu verfügen und so eine Ausbildungskontrolle (vgl. Artikel 127 Buchstabe d MIG) und das Kompetenzmanagement (vgl. Artikel 127 Buchstabe g MIG) zu ermöglichen, ist es erforderlich, die Aufbewahrungsdauer derart zu verlängern, dass die Daten des LMS VBS noch bis zehn Jahre nach der Entlassung aus der Militärdienstpflicht bzw. nach Beendigung des Arbeitsverhältnisses aufbewahrt werden können. Dadurch werden die betroffenen Personen auch davon befreit, erforderliche Ausbildungen nochmals machen oder Fähigkeitsnachweise nochmals einreichen zu müssen.

Gliederungstitel vor Art. 138, Art. 138, 139 Einleitungssatz sowie Bst. a, c, e und f, 140 Einleitungssatz und Bst. b, 141 Einleitungssatz sowie Bst. b, c, d und e, 142 Abs. 1 sowie 143 (Informationssystem MIFA)

Das Strassenverkehrs- und Schifffahrtsamt der Armee (SVSAA) ist unter anderem zuständig für die Erstellung, die Verwaltung und den Entzug:

- der militärischen Fahrberechtigungen für Fahrzeug- (vgl. Artikel 32 und 38 der Verordnung vom 11. Februar 2004¹⁵ über den militärischen Strassenverkehr [VMSV]) und Schiffsführerinnen und -führer (vgl. Artikel 4 und 14 der Verordnung vom 1. März 2006¹⁶ über die militärische Schifffahrt [VMSch]),

¹⁵ SR 510.710

¹⁶ SR 510.755

-
- der Ausweise der militärischen Verkehrsexpertinnen und -experten (bzw. Prüfungsexpertinnen und -experten), welche Prüfungen für Fahrzeug- (vgl. Artikel 29 VMSV) und Schiffsführerinnen und -führer (vgl. Artikel 4 VMSch) abnehmen, sowie
 - der eidgenössischen Schiffsführerinnen- und Schiffsführerausweise (vgl. Artikel 3 und 11 der Verordnung vom 1. März 2006¹⁷ über die zivile Schifffahrt der Bundesverwaltung).

Die für die Erfüllung dieser Aufgaben erforderlichen Personendaten sollen alle in dem vom SVSAA betriebenen Informationssystem bearbeitet werden. Entsprechend ist die heutige, inhaltlich zu wenig weit gehende Beschreibung «Informationssystem Militärische Fahrberechtigung» (abgekürzt: «MIFA») allgemeiner zu fassen und in «Informationssystem Strassenverkehr und Schifffahrt der Armee» (abgekürzt: «FA-SVSAA») [für «Fachanwendung Strassenverkehrs- und Schifffahrtsamt der Armee»] abzuändern. Ebenfalls zu ergänzen sind die vorgenannten Personengruppen bzw. Fahrberechtigungen und Ausweise – soweit noch nicht aufgeführt – in der Zweckbestimmung (Artikel 139 Buchstaben a und c) und in der Bestimmung mit den zu bearbeitenden Personendaten (Artikel 140 Buchstabe b). Ferner ist zudem als neue Datenbeschaffungsquelle insbesondere für Daten betreffend Eidgenössische Schiffsführerausweise das IPDM (vgl. Artikel 30–38 BPDV) in Artikel 141 Buchstabe d zu nennen.

Ebenfalls in der Zweckbestimmung ist der bestehende Artikel 139 Buchstabe f aufzuheben, da heute keine Daten mehr zu diesem dort genannten Zweck bearbeitet werden.

Die in Artikel 141 Buchstabe b als Datenbeschaffungsquellen bzw. in Artikel 142 Absatz 1 Buchstabe b als Datenempfänger genannten Register (Fahrberechtigungsregister und Administrativmassnahmenregister) wurden durch das vom Bundesamt für Strassen betriebene Informationssystem Verkehrszulassung (IVZ; vgl. hierzu die Verordnung vom 30. November 2018¹⁸ über das Informationssystem Verkehrszulassung) abgelöst und sind entsprechend zu ersetzen.

In Artikel 143 Absatz 1 soll die Aufbewahrung der Daten des FA-SVSAA, einschliesslich Daten über militärische Administrativmassnahmen, nicht mehr nur bis zur Entlassung der betreffenden Person aus der Militärdienstpflicht, sondern bis 80 Jahre nach der Erfassung der Daten möglich sein. Dies ist deshalb erforderlich, da militärische Fahrberechtigungen etwa gemäss Artikel 33 VMSV auch nach dem Ausscheiden einer Fahrzeugführerin oder eines Fahrzeugführers aus der Armee ihre Gültigkeit für die ausserdienstliche militärische Tätigkeit behalten. Weiter sind bereits heute zahlreiche militärische Verkehrsexpertinnen und -experten nicht mehr militärdienstpflichtig. Aus diesen Gründen muss das SVSAA auch über den Zeitpunkt der Entlassung einer betreffenden Person aus der Militärdienstpflicht hinaus seine Verwaltungs- und Kontrollaufgabe ausüben und über die hierfür nötigen Personendaten verfügen können. Dies wird zusätzlich dadurch unterstützt, dass in Artikel 141 Buchstabe c als weitere Datenbeschaffungsquelle das IPV anzuführen ist, aus dem insbesondere – anders als aus dem PISA – aktuelle Daten bezogen

¹⁷ SR 747.201.2

¹⁸ SR 741.58

werden können zu den Ausweisen von militärischen Verkehrsexpertinnen und -experten, die nicht mehr militärdienstpflichtig sind. Abweichend von Artikel 143 Absatz 1 werden die in der FA-SVSAA bearbeiteten Daten über zivile Administrativmassnahmen (Art der Administrativmassnahme, ihr Grund, ihre Dauer sowie die Stelle, welche die Administrativmassnahme verfügt und/oder erfasst hat) nach Artikel 143 Absatz 2 nur solange aufbewahrt, wie sie im IVZ enthalten sind. Bei den in Artikel 143 Absatz 3 ferner genannten Kontrolluntersuchungen ist für das SVSAA nur relevant, wann und mit welchem Ergebnis zuletzt eine Kontrolluntersuchung stattgefunden hat und wie lange dieses Ergebnis gültig ist, das heisst wann die Kontrolluntersuchung künftig wiederholt werden muss; die Daten zu weiter zurückliegenden Kontrolluntersuchungen müssen nicht aufbewahrt werden.

Weitere Änderungen betreffen die Artikel 139 Buchstabe e und 140 Einleitungssatz (jeweils geschlechtergerechte Formulierung) sowie 141 Buchstabe e und 142 Absatz 1 Buchstabe a (der Einheitlichkeit halber Nennung von «Stellen und Personen» anstatt «Personen und Stellen» wie in zahlreichen anderen Bestimmungen des MIG).

Art. 147 Abs. 2 Bst. d sowie 148 Abs. 1 Bst. c Ziff. 2^{bis} und Bst. d (Informationssystem SIBAD)

Die Rechtsgrundlagen für einen Zugriff durch Abrufverfahren auf Daten aus diversen Datenbanken der Zentralstelle Waffen nach Artikel 32a Absatz 1 des Bundesgesetzes vom 20. Juni 1997¹⁹ über Waffen, Waffenzubehör und Munition (Waffengesetz, WG) (Waffeninformationsplattform ARMADA) existieren bereits. Sie befinden sich in Artikel 32c Absatz 8 WG i.V.m. Artikel 61 Absatz 2 Buchstabe e und Artikel 61 Absatz 6 i.V.m. Anhang 3 der Verordnung vom 2. Juli 2008²⁰ über Waffen, Waffenzubehör und Munition (Waffenverordnung, WV). Entsprechend soll diese Möglichkeit des Zugangs durch Abrufverfahren auch in Artikel 147 Absatz 2 Buchstabe d aufgenommen werden. Auf eine Nennung der einzelnen Datenbanken der Zentralstelle Waffen in Artikel 147 Absatz 2 Buchstabe d, auf welche zugegriffen werden darf, ist zu verzichten, zumal der Einleitungssatz des Artikels 147 Absatz 2 den Umfang des Zugangs durch Abrufverfahren von den «entsprechenden Rechtsgrundlagen» abhängig macht und so allfällige Anpassungen der Zugriffsrechte etwa auf Verordnungsstufe in der Waffenverordnung ohne weitere gesetzliche Anpassungen im MIG automatisch auch mit Bezug auf das SIBAD gelten würden.

Weiter ist in Artikel 148 Absatz 1 Buchstabe c Ziffer 2^{bis} die nationale Netzgesellschaft aufzuführen, da gemäss dem am 1. Januar 2018 in Kraft getretenen Artikel 20a des Bundesgesetzes vom 23. März 2007²¹ über die Stromversorgung (Stromversorgungsgesetz, StromVG) auch Personen, die bei der nationalen Netzgesellschaft mit gewissen Aufgaben betraut sind, einer Personensicherheitsprüfung unterzogen werden sollen. Mittels des Zugangs der nationalen Netzgesellschaft auf das SIBAD durch Abrufverfahren wird die an diese erfolgende, in Artikel 20a Absatz 3 StromVG vorgesehene Mitteilung der Ergebnisse der Personensicherheitsprüfungen erleichtert. Die nationale Netzgesellschaft könnte selber die Daten aus dem SIBAD

¹⁹ SR 514.54

²⁰ SR 514.541

²¹ SR 734.7

abrufen, wobei im Sinne des gemäss Artikel 1 Absatz 3 MIG i.V.m. Artikel 4 Absatz 2 DSGVO geltenden Verhältnismässigkeitsgrundsatzes nur diejenigen Daten abrufbar sein würden, welche die nationale Netzgesellschaft zur Erfüllung ihrer Aufgabe benötigt.

Mit der Ergänzung in Artikel 148 Absatz 1 Buchstabe d soll sichergestellt werden, dass die Daten des SIBAD und somit der Personensicherheitsprüfungen nur solchen, mit Sicherheitsaufgaben beauftragten Stellen des Bundes durch Abrufverfahren zugänglich sind, die für ihre Tätigkeit auf diesen Daten basieren müssen. Zudem soll auch nur der Zugang auf die für die betreffende Person nicht nachteiligen Daten möglich sein.

Gliederungstitel vor Art. 167a, Art. 167a, 167b Bst. a und b, 167d, 167e Abs. 1 und 2 Bst. b und c sowie 167f (Informationssystem JORASYS)

Der Name des JORASYS ist den mit der WEA geschaffenen neuen Organisationsstrukturen anzupassen (neu «Journal- und Rapportsystem der Militärpolizei» anstatt «Journal- und Rapportsystem der Militärischen Sicherheit»).

In Artikel 167d Buchstabe e ist einerseits die Regelung des bisherigen Artikels 167d Absatz 2 MIG integriert, wobei für das MIFA die neu einzuführende Abkürzung FA-SVSAA (vgl. hierzu Artikel 138 ff. und die vorstehenden zugehörigen Erläuterungen) zu verwenden ist. Weiter soll im Einleitungssatz des Artikels 167d Buchstabe e explizit geregelt werden, dass die Datenbeschaffung aus allen, unter Artikel 167d Buchstabe e genannten Informationssystemen (insbesondere auch den unter Ziffern 2–7 und 9 neu Aufgenommenen) manuell durch Abrufverfahren (in der Regel über eine von den Betreibern des jeweiligen Informationssystems bereitgestellte Web-Schnittstelle oder über eine spezifische Software) oder auch automatisiert über eine (geplante) Schnittstelle, über welche die Daten automatisch übernommen werden können, möglich ist. Dadurch kann die Beschaffung der Personendaten, die für die tägliche Aufgabenerfüllung (z. B. etwa für die Erstellung von Berichten zuhanden der Justiz, die Vorbereitung von Interventionen oder die Durchführung von Kontrollen durch die Militärverkehrspolizei) erforderlich sind und stets aktuell zur Verfügung stehen sollten, beschleunigt und vereinfacht werden. Im Einzelnen gewähren die neu in Artikel 167d Buchstabe e aufgenommenen Informationssysteme Zugang zu den folgenden Daten:

(Neu aufgenommenes) Informationssystem	Gewährt Zugang zu folgenden Daten:
RIPOL (Artikel 167d Buchstabe e Ziffer 2)	Daten zu ungeklärten Straftaten (z. B. als gestohlen gemeldete Gegenstände) (vgl. Artikel 3 Buchstabe h, 6 Absatz 1 Buchstabe o, 7 Absatz 1 sowie Anhang 1 Tabellenziffer 2 der Verordnung vom 26. Oktober 2016 ²² über das automatisierte Polizeifahndungssystem [RIPOL-Verordnung])

IVZ (Artikel 167d Buchstabe e Ziffer 3)	Daten zu Fahrzeugen und deren Verkehrszulassung, zu Fahrzeugführerinnen und -führern sowie deren Fahrberechtigung, zu Fahrzeughalterinnen und -haltern sowie zu Motorfahrzeugversicherungen (vgl. Artikel 89e Buchstabe a des Strassenverkehrsgesetzes vom 19. Dezember 1958 ²³ [SVG])
Datenbanken der Zentralstelle Waffen nach Artikel 32a WG (Artikel 167d Buchstabe e Ziffer 4)	Online-Zugang zu den Daten der Datenbanken der Zentralstelle Waffen nach Artikel 32a WG, um zu überprüfen, ob einer Person der Erwerb von Waffen untersagt oder ihr die Waffe abgenommen wurde (vgl. Artikel 32a–32c WG)
Online-Abfrage Waffenregister der Kantone (Artikel 167d Buchstabe e Ziffer 5)	Online-Abfrage in den kantonalen Registern der Feuerwaffenbesitzer (Daten über den Erwerb und Besitz von Feuerwaffen) (vgl. Artikel 32a Absätze 2 und 3 sowie 32b Absatz 6 WG)
PISA (Artikel 167d Buchstabe e Ziffer 6)	Militärische Daten wie Einteilung, Grad, Funktion und Dienstleistungen in der Armee (vgl. Artikel 167c Absatz 1 Buchstabe d)
IPV (Artikel 167d Buchstabe e Ziffer 7)	Daten wie Funktion, Ausbildung, Einsatz in der Armee, militärischer Status, berufliche Laufbahn, Sprachkenntnisse (vgl. Artikel 62 Buchstaben b–e und g MIG)
DDSV (Artikel 167d Buchstabe e Ziffer 9)	Daten wie Einteilung, Grad, Funktion, Ausbildung, Qualifikation und Ausrüstung in der Armee und im Zivilschutz (vgl. Artikel 176 Buchstabe a MIG)

Zumal Artikel 100 des Bundesgesetzes vom 3. Februar 1995²⁴ über die Armee und die Militärverwaltung (Militärgesetz, MG) mehrere Aufgaben (und nicht nur eine) nennt, die von den Mitarbeiterinnen und Mitarbeitern des Kommandos Militärpolizei zu erfüllen sind, ist in Artikel 167e Absatz 1 Buchstabe b eine entsprechende Anpassung des in der Einzahl («Aufgabe») verwendeten Begriffs vorzunehmen. Weiter sind in Artikel 167e Absatz 1 Buchstabe c der Einfachheit und Klarheit halber die Mitarbeiterinnen und Mitarbeiter des DPISA zu nennen, bei denen es sich um die im heutigen Wortlaut umschriebenen Personen handelt, die mit der Beurteilung der militärischen Sicherheitslage und dem Eigenschutz der Armee beauftragt sind (vgl. nur Artikel 100 Absatz 1 Buchstaben a und e MG sowie Artikel 11 der Verordnung vom 21. November 2018²⁵ über die Militärische Sicherheit [VMS]). Der Artikel 167e Absatz 2 Buchstabe b ist geschlechtermäßig zu formulieren. In Artikel 167e Absatz 2 Buchstabe c ist nicht eine bestimmte, für die Informations- und Objektsicherheit zuständige Stelle (wie etwa die organisatorisch dem General-

23 SR 741.01

24 SR 510.10

25 SR 513.61

sekretariat des VBS zugehörige Informations- und Objektsicherheit) zu nennen, sondern es sollen sämtliche, für die Informations- und Objektsicherheit zuständigen Stellen (insbesondere auch diejenigen innerhalb der Gruppe Verteidigung) als mögliche Datenempfänger vom Wortlaut erfasst sein. Ferner wird eine einheitliche, nach Abschluss der militärpolizeilichen Tätigkeit zu einem Vorfall beginnende zehnjährige Aufbewahrungsfrist für beschaffte Daten als hinreichend wie auch erforderlich erachtet, weshalb Artikel 167*f* entsprechend anzupassen ist.

Die Änderungen in Artikel 167*b* Buchstaben a und b sowie in Artikel 167*e* Absatz 1 Einleitungssatz und Buchstabe a sind rein sprachlicher Natur und betreffen nur den französischen Wortlaut.

(5. Kapitel) / 6. Abschnitt (Art. 167g–167l) (Informationssystem IPSA)

Mit den neu einzuführenden Artikeln 167g–167l soll eine Rechtsgrundlage für das dem DPSA zur Erfüllung seiner Aufgaben, insbesondere zur Beurteilung der militärischen Sicherheitslage und zum vorsorglichen Schutz der Armee vor Spionage, Sabotage und weiteren rechtswidrigen Handlungen (vgl. Artikel 100 Absatz 1 Buchstaben a und e MG sowie Artikel 11 VMS), sowie zur Journal- und Einsatzführung dienende IPSA geschaffen werden. Um die vorgenannten Aufgaben optimal erfüllen zu können, ist es notwendig, die im Zusammenhang mit einer möglichen Bedrohung der Armee stehenden Personen (Artikel 167*i* Einleitungssatz) samt Detailangaben zu dieser Bedrohung (Artikel 167*i* Buchstabe m) im IPSA erfassen zu können.

Da im IPSA auch besonders schützenswerte Personendaten (vgl. etwa Artikel 167*i* Buchstaben c [ethnische und religiöse Zugehörigkeit, benötigt für die Einschätzung möglicher Motive in den Bereichen Gewaltextremismus, Terrorismus und Spionage gegen die Armee], e [politische und ideologische Ausrichtung, benötigt für die Einschätzung möglicher Motive in den Bereichen Gewaltextremismus, Terrorismus und Spionage gegen die Armee] und h [medizinische und biometrische Daten, benötigt etwa für die eindeutige Identifizierung von Personen oder für die Erfassung psychischer Erkrankungen, die einen Einfluss auf die Sicherheit der Armee haben könnten], und n [weitere, auch besonders schützenswerte Personendaten {vgl. Artikel 100 Absatz 3 Buchstabe a MG}]) und Persönlichkeits(teil)profile (vgl. etwa Artikel 167*i* Buchstaben k [Daten über den Aufenthaltsort der Person, einschliesslich Bewegungsprofilen] und l [Daten über die von der Person verwendeten Fortbewegungs- und Kommunikationsmittel, einschliesslich Nutzungs- und Standortdaten sowie Bewegungsprofilen], und n [weitere Persönlichkeitsprofile {vgl. Artikel 100 Absatz 3 Buchstabe a MG}] für die Aufgabenerfüllung bearbeitet werden müssen, bedarf es gemäss Artikel 17 Absatz 2 DSGVO einer Rechtsgrundlage in einem formellen Gesetz.

Bei den Bezugspersonen, deren Daten und Identitäten im IPSA ebenfalls bearbeitet werden (Artikel 167*i* Buchstabe j), handelt es sich um Personen, die zwar selbst keine Bedrohung für die Armee darstellen müssen, die jedoch einen Bezug zu einer Person aufweisen, die im Zusammenhang mit einer möglichen Bedrohung der Armee steht. Solche Bezugspersonen können dazu dienen, Personen mit Bedrohungspotenzial zu erkennen, aufzufinden oder anzusprechen, um dadurch eine Bedrohung zu vermindern oder sogar zu verhindern.

Die Datenbeschaffung soll nebst den unter Artikel 167j Buchstaben a–f genannten Quellen auch durch Abrufverfahren aus den unter Artikel 167j Buchstabe g genannten Informationssystemen permanent möglich sein, damit der DPSA die zur Aufgabenerfüllung erforderlichen Personendaten jederzeit schnell und einfach beschaffen kann.

Art. 168, 169 Einleitungssatz sowie Bst. d und e, 170 Einleitungssatz sowie Bst. a und a^{bis}, 171 Einleitungssatz und Bst. i, 172 und 173 (Informationssystem SCHAWÉ)

Das Generalsekretariat des VBS arbeitet mit der Nachfolganwendung des seit Ende 2003 betriebenen SCHAWÉ. Die technische Bezeichnung der neuen Anwendung lautet SCHAMIS; sie ist abgeleitet aus «SCHA(den)M(anagement)» und «I(nformations)S(ystem)». Im ganzen Erlass hat eine Anpassung dieses Kürzels zu erfolgen.

In Artikel 169 Buchstaben d und e sind zwei neue Zwecke, denen das SCHAMIS dient, festzuhalten:

- Zum einen erfolgt die Schadenregulierung bei Unfällen und Schadenfällen im Zusammenhang mit Bundesfahrzeugen nach Artikel 21 der Verordnung vom 23. Februar 2005²⁶ über die Fahrzeuge des Bundes und ihre Führer und Führerinnen durch das Schadenzentrum VBS. Als Folge dieser versicherungsähnlichen Tätigkeit stellt es auch die elektronischen Versicherungsnachweise für die Bundesfahrzeuge nach Artikel 5 Absatz 1 Buchstabe b der Verkehrsversicherungsverordnung vom 20. November 1959²⁷ zu Handen der kantonalen Fahrzeugzulassungsstellen (Strassenverkehrsämter) aus. Neu kann dieser Arbeitsschritt über die Anwendung SCHAMIS verarbeitet und daher in die Zweckbestimmung des Gesetzes (Artikel 169 Buchstabe d) aufgenommen werden.
- Zum anderen wird die Regulierung von Schadenfällen von Motorfahrzeugen von Ratsmitgliedern nach Artikel 4 Absatz 2 der Verordnung der Bundesversammlung vom 18. März 1988²⁸ zum Parlamentsressourcengesetz wird über die Anwendung SCHAMIS abgewickelt, was in der entsprechenden Zweckbestimmung des Gesetzes (Artikel 169 Buchstabe e) festzuhalten ist.

Die aus datenschutzrechtlichen Gründen notwendige gesetzliche Grundlage des Informationssystems des Schadenzentrums VBS machte es schon bisher möglich, Angaben zu Schadenereignissen zu bearbeiten. Um den Anforderungen des modernen Datenschutzgedankens nachzukommen, drängt es sich auf, diese Angaben in Artikel 170 Buchstabe a zu präzisieren und zudem die Bearbeitung besonders schützenswerter Personendaten von Geschädigten und Schädigenden wie Angaben über die Finanzverhältnisse und Straf-, Zivil-, Disziplinar- und Verwaltungsverfahren bereits im Gesetz ausdrücklich zu benennen. Bewusst wird neu auch die auf ein zweckmässiges Minimum reduzierte Bearbeitung von Daten von Dritten geregelt (vgl. Artikel 170 Buchstabe a^{bis}).

26 SR 514.31

27 SR 741.31

28 SR 171.211

Bei der Regulierung von Schadenfällen tauschen private Versicherungen unter sich verschiedenste Daten aus, beispielsweise um die Schuldfrage anhand von Verfahrensakten zu klären oder Regressforderungen betragsmässig zu belegen. Dass auch das wie eine Versicherung handelnde Schadenzentrum VBS direkt bei Versicherungen Daten beschafft, war bisher im Gesetz nur implizit vorgesehen, indem Daten über die betroffenen Personen oder über Referenzpersonen beschafft werden durften. Neu sollen die Versicherungen in Artikel 171 Buchstabe i explizit verankert werden.

Bei der Erledigung von Schadenfällen müssen in vielen Fällen Dritten Daten bekannt gegeben werden. Diese Dritten handeln formell nicht immer im Auftrag des Generalsekretariates respektive des Schadenzentrums VBS, weshalb diese unnötige Einschränkung in Artikel 172 Absatz 2 entfällt.

Gliederungstitel vor Art. 174, Art. 174, 175 Einleitungssatz, 176 Einleitungssatz und Bst. c, 177 Einleitungssatz, 178 und 179 (Informationssystem SISLOG)

Bezeichnung und Abkürzung des Informationssystems sind in Anpassung an die zukünftige Systemlösung sowie entsprechend dem mit ihm hauptsächlich verfolgten Zweck einer Datendrehschreibe von «Strategisches Informationssystem Logistik (SISLOG)» zu «Datendrehscheibe Verteidigung (DDSV)» zu ändern. Genutzt wird das Informationssystem DDSV heute auch ausserhalb der Logistikbasis der Armee (LBA) in der Gruppe Verteidigung.

Zu den Daten nach Artikel 176 Buchstabe c, die mit dem DDSV beim Datenaustausch zwischen militärischen Informationssystemen nach Artikel 175 Buchstabe c MIG auszutauschen sind, gehören auch besonders schützenswerte Personendaten und Persönlichkeitsprofile (vgl. die Definition des Begriffs «Daten» in Artikel 1 Absatz 1 MIG).

In Artikel 178 ist näher differenzierend zu präzisieren, welche im DDSV bearbeiteten Personendaten welchen Stellen und Personen bekannt gegeben werden dürfen. So sollen die im DDSV für den Datenaustausch zwischen den militärischen Informationssystemen bearbeiteten Personendaten nur denjenigen Stellen und Personen bekannt gegeben werden, die auch für die vom Datenaustausch jeweils betroffenen militärischen Informationssysteme zuständig sind. Einzig die Personendaten nach Artikel 176 Buchstaben a und b MIG sind für die Bekanntgabe an militärische Kommandos sowie an zuständige Verwaltungseinheiten des Bundes und der Kantone gedacht.

Art. 179b Bst. d, 179c Abs. 4, 179d Bst. e und 179e Abs. 2 Bst. e (Informationssystem PSN)

Anstelle der beiden nicht mehr existierenden, aufgehobenen Artikel, auf die verwiesen wird, soll in Artikel 179c Absatz 4 lediglich noch in unspezifischer Weise auf das Bundespersonalgesetz vom 24. März 2000²⁹ und dessen Ausführungsbestim-

²⁹ SR 172.220.1

mungen (vgl. Artikel 8 ff. BPDV für das Bewerbungsdossier und Artikel 19 ff. BPDV für das Personaldossier) verwiesen werden.

Da das BV PLUS durch das neu in den Artikeln 30–38 BPDV geregelte IPDM abgelöst wurde, ist zudem in den Artikeln 179*d* Buchstabe e und 179e Absatz 2 Buchstabe e das IPDM anstelle des BV PLUS zu nennen.

Die Änderung des Artikels 179*b* Buchstabe d ist bloss formeller Art und rechtsetzungstechnisch bedingt (Verwendung der bereits zuvor in Artikel 16 Absatz 3^{bis} eingeführten Abkürzung «WG»); sie betrifft nur den deutschen Wortlaut.

(6. Kapitel) / 5. Abschnitt (Art. 179m–179r) (Informationssystem MDM)

In den neu einzufügenden Artikeln 179*m*–179*r* soll eine Rechtsgrundlage für das vom Generalsekretariat des VBS zu betreibende MDM geschaffen werden. Mit dem MDM sollen für das gesamte VBS einheitliche und eindeutige Daten von bestehenden und auch erst künftig möglichen, etwa an einem Vertragsabschluss interessierten Geschäftspartnerinnen und Geschäftspartnern (vgl. Artikel 179*o*) für die Geschäftsprozesse in den Bereichen Finanzen, Beschaffung, Logistik, Immobilien und Personal verwaltet und bereitgestellt werden (Artikel 179*n*) – sogenannte «Stammdaten» (bzw. «Master Data»). Zu diesen Daten gehört auch die «Sozialversicherungsnummer» (Artikel 179*o* Buchstabe k), worunter sowohl die AHV-Versichertennummer als auch ausländische Sozialversicherungsnummern von Geschäftspartnerinnen und Geschäftspartnern aus dem Ausland fallen. Geschäftspartnerinnen und Geschäftspartner können sowohl Privatpersonen als auch Unternehmen sein. Die Bewirtschaftung der vordefinierten Stammdaten erfolgt zentral und ausschliesslich über das MDM, damit der Zweck einer Stammdatenquelle mit höchstmöglicher Datenqualität und Aktualität erfüllt werden kann. Aufgrund erhöhter Sicherheits- und Informationsschutzbedürfnissen innerhalb des VBS soll das Master-Data-Management über ein eigenes Informationssystem und nicht über dasjenige des Bundes (ohne VBS), welches beim Eidgenössischen Finanzdepartement (EFD) angesiedelt ist, betrieben werden; vorwiegend aus Letzterem sind jedoch über eine Schnittstelle die bundesweit eindeutigen (sogenanntes «once-only-Prinzip»), nicht verwaltungsspezifisch angereicherten Daten für das MDM zu beschaffen (vgl. Artikel 179*p* Buchstabe c). Die weitere Bekanntgabe der Daten des MDM innerhalb des VBS soll durch Abrufverfahren erfolgen. Bei der Regelung der Datenaufbewahrung ist bei den mit einer Geschäftspartnerin oder einem Geschäftspartner verknüpften logistischen Stammdaten (wie Materialstammdaten und Systemstrukturdaten) in Abhängigkeit des Lebenszyklus etwa eines Materialstamms nach Beendigung der Geschäftsbeziehung zu einer Geschäftspartnerin oder einem Geschäftspartner eine Aufbewahrungsdauer von fünfzig Jahren (und nicht – wie bei allen übrigen Daten der Geschäftspartnerinnen oder Geschäftspartnern – von nur zehn Jahren gemäss Vorgabe des Bundesgesetzes vom 7. Oktober 2005³⁰ über den eidgenössischen Finanzhaushalt und dessen Ausführungsbestimmungen) vorzusehen (Artikel 179*r* Absatz 1 Buchstabe b). Steht fest, dass eine Person, die zunächst als künftig mögliche Geschäftspartnerin bzw. künftig möglicher Geschäftspartner im MDM erfasst wurde, nun doch nicht Ge-

schäftspartnerin oder Geschäftspartner wird, sind deren Daten ab diesem Zeitpunkt nur während zwei Jahren aufzubewahren (Artikel 179r Absatz 2).

Art. 181 Abs. 1 Bst. a und Abs. 2 Einleitungssatz (Überwachungsmittel)

Durch die Erweiterung des in Artikel 181 Absatz 1 Buchstabe a festgehaltenen Zwecks soll es neu möglich sein, Überwachungsmittel auch für die Überwachung militärisch genutzter Objekte der Armee, der Militärverwaltung oder von Dritten – so etwa auch von zivilen Liegenschaften der LBA, in denen Armeematerial gelagert wird – einzusetzen und die hierzu nötigen Personendaten zu beschaffen und weiter zu bearbeiten.

Mit der Anpassung des Einleitungssatzes von Artikel 181 Absatz 2 soll berichtend bzw. präzisierend verdeutlicht werden, dass die Armee den zivilen Behörden auf Gesuch hin nie luftgestützte Überwachungsmittel mitsamt Personal zur Verfügung stellt (im Sinne von überlässt), sondern lediglich luftgestützte Überwachungsleistungen zu Gunsten der zivilen Behörden erbringen kann.

Art. 186 Abs. 3

Um internationale Abkommen, die als Rechtsgrundlage für eine grenzüberschreitend erfolgende Bearbeitung von nicht besonders schützenswerten Personendaten dienen (vgl. hierzu auch die Erläuterungen zu Artikel 6 Buchstabe b), abschliessen zu dürfen, soll dem Bundesrat in Artikel 186 Absatz 3 die entsprechende Kompetenz eingeräumt werden.

4 Auswirkungen

4.1 Finanzielle, personelle und andere Auswirkungen auf den Bund

Die beantragten Anpassungen im MIG haben keine finanziellen, personellen oder anderen Auswirkungen auf den Bund. Mit ihnen werden lediglich die datenschutzrechtlich verlangten Rechtsgrundlagen geschaffen für die Legitimation derjenigen Bearbeitungen von Personendaten, die für die Erfüllung der öffentlichen Aufgaben ohnehin erforderlich sind und erfolgen müssen. Allfällige nötige Arbeiten insbesondere (informatik-)technischer Natur erfolgen im Rahmen der laufenden Systemanpassungen und -(weiter)entwicklungen.

4.2 Weitere Auswirkungen

Die Massnahmen und Anpassungen des vorliegenden Berichts haben keine weiteren Auswirkungen etwa auf die Kantone und Gemeinden, auf urbane Zentren, Agglomerationen und Berggebiete, auf die Volkswirtschaft, auf die Gesellschaft und auf die Umwelt.

5 Rechtliche Aspekte

5.1 Verfassungsmässigkeit

Mit Bezug auf die im MIG bereits geregelten militärischen Informationssysteme stützt sich die Regelungskompetenz des Bundes, wie dies auch aus dem bestehenden Ingress des MIG hervorgeht, insbesondere auf Artikel 60 Absatz 1 BV, der die Militärgesetzgebung sowie Organisation, Ausbildung und Ausrüstung der Armee als Sache des Bundes bezeichnet, und – mit Bezug auf die Bearbeitung von Personendaten von Auslandschweizerinnen und Auslandschweizern – auch auf Artikel 40 Absatz 2 BV. Für die neu explizit in den Geltungsbereich des MIG aufzunehmenden nicht militärischen Informationssysteme des VBS ist mangels Vorhandensein einer expliziten Kompetenznorm auf Artikel 173 Absatz 2 BV abzustützen. Denn die nicht militärischen Informationssysteme (sowie die in diesen erfolgenden Bearbeitungen von Personendaten) dienen der Wahrnehmung von anderweitig verankerten Bundesaufgaben, welche das VBS erfüllen muss. Ihre Regelung beschlägt daher letztlich eine Frage der Organisation der Verwaltungseinheiten des VBS, wofür diese bzw. der Bund selbst zuständig sind.

5.2 Vereinbarkeit mit internationalen Verpflichtungen der Schweiz

Die beantragten Gesetzesänderungen sind mit den völkerrechtlichen Verpflichtungen der Schweiz vereinbar. Sie schaffen auch keine neuen Verpflichtungen der Schweiz gegenüber andern Staaten oder internationalen Organisationen.

5.3 Erlassform

Im vorliegenden Fall handelt es sich um wichtige rechtsetzende Normen im Sinne von Artikel 164 BV, die in einem formellen Gesetz festzuhalten sind. Zudem erfordert die in diesen Normen unter anderem vorgesehene Bearbeitung von besonders schützenswerten Personendaten nach Artikel 17 Absatz 2 DSG eine Grundlage in einem formellen Gesetz.

5.4 Unterstellung unter die Ausgabenbremse

Die beantragten Gesetzesänderungen unterstehen nicht der Ausgabenbremse nach Artikel 159 Absatz 3 Buchstabe b BV, da sie weder Subventionsbestimmungen noch die Grundlage für die Schaffung eines Verpflichtungskredits oder Zahlungsrahmens enthalten.

5.5 Einhaltung des Subsidiaritätsprinzips und des Prinzips der fiskalischen Äquivalenz

Das Subsidiaritätsprinzip und das Prinzip der fiskalischen Äquivalenz sind von den beantragten Gesetzesänderungen nicht betroffen.

5.6 Einhaltung der Grundsätze der Subventionsgesetzgebung

Die beantragten Gesetzesänderungen sehen keine Finanzhilfen oder Abgeltungen im Sinne des Subventionsgesetzes vom 5. Oktober 1990³¹ vor.

5.7 Delegation von Rechtsetzungsbefugnissen

Rechtsetzungsbefugnisse können durch Bundesgesetz übertragen werden, soweit dies nicht durch die Bundesverfassung ausgeschlossen wird (Artikel 164 Absatz 2 BV). In Artikel 186 Absatz 3 des vorliegenden Entwurfs soll dem Bundesrat die Kompetenz für den Abschluss von internationalen Abkommen über die grenzüberschreitende Bearbeitung von nicht besonders schützenswerten Personendaten eingeräumt werden. Weiter ist der Bundesrat befugt, gestützt auf den bestehenden Artikel 186 Absatz 1 MIG auch zu den neu einzuführenden Informationssystemen die erforderlichen Ausführungsbestimmungen zu erlassen.

5.8 Datenschutz

Nach Artikel 17 Absatz 2 DSG dürfen Organe des Bundes besonders schützenswerte Personendaten sowie Persönlichkeitsprofile nur dann bearbeiten und nach Artikel 19 Absatz 3 DSG dürfen Daten nur durch ein Abrufverfahren zugänglich gemacht werden, wenn ein Gesetz im formellen Sinn dies ausdrücklich vorsieht. Um die für die Aufgabenerfüllung notwendige Bearbeitung und den Austausch von Personendaten sicherzustellen, bedarf es aus datenschutzrechtlicher Sicht der in diesem Bericht vorgesehenen Anpassungen bestehender Rechtsgrundlagen.

³¹ SR 616.1