Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

21.xxx

Botschaft zur Änderung des Bundesgesetzes über die militärischen Informationssysteme

vom …

Sehr geehrter Herr Nationalratspräsident
Sehr geehrter Herr Ständeratspräsident
Sehr geehrte Damen und Herren

Mit dieser Botschaft unterbreiten wir Ihnen, mit dem Antrag auf Zustimmung, den Entwurf einer Änderung des Bundesgesetzes über die militärischen Informationssysteme.

Wir versichern Sie, sehr geehrter Herr Nationalratspräsident, sehr geehrter Herr Ständeratspräsident, sehr geehrte Damen und Herren, unserer vorzüglichen Hochachtung.

…

Im Namen des Schweizerischen Bundesrates

Der Bundespräsident: Guy Parmelin
Der Bundeskanzler: Walter Thurnherr

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, damit die für die Aufgabenerfüllung nötigen Personendaten auch künftig zur Verfügung stehen.

Ausgangslage

Die Bedürfnisse des VBS im Zusammenhang mit der für eine optimale Aufgabenerfüllung notwendigen Bearbeitung von Personendaten in seinen Informationssystemen haben sich – insbesondere auch infolge der «Weiterentwicklung der Armee» (WEA) – verändert. Damit Personendaten entsprechend diesen neuen Bedürfnissen rechtmässig bearbeitet werden dürfen, setzt das Datenschutzrecht das Bestehen einer hinreichenden gesetzlichen Grundlage voraus. Diese datenschutzrechtlich notwendigen gesetzlichen Grundlagen enthält das MIG noch nicht. Daher sind 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 sowie Bestimmungen für neue Informationssysteme in das MIG aufzunehmen. Diese Änderungen betreffen insbesondere:

- *die Bearbeitung von neuen Personendaten,*
- *die Bearbeitung von Personendaten zu neuen Bearbeitungszwecken,*
- *die Beschaffung von Personendaten bei weiteren Stellen, Personen und Informationssystemen,*
- *die Bekanntgabe von Personendaten an weitere Stellen, Personen und Informationssysteme,*
- *die Zusammenlegung bestehender Informationssysteme,*
- *die Neuregelung der für die Informationssysteme verantwortlichen Organe,*
- *die Umbenennung von Informationssystemen,*
- *die erleichterte Datenübermittlung mittels Abrufverfahren, Schnittstellen und elektronischer Portale,*
- *die Neuregelung der Dauer der Datenaufbewahrung.*

Inhaltsverzeichnis

Botschaft

1 Ausgangslage

1.1 Handlungsbedarf und Ziele

Die Gruppe Verteidigung und die ihr unterstellten Verwaltungseinheiten betreiben diverse militärische Informationssysteme. Die Bearbeitung von Personendaten in diesen Informationssystemen wird im Bundesgesetz vom 3. Oktober 2008[1] über die militärischen Informationssysteme (MIG) geregelt. Darüber hinaus enthält das MIG Bestimmungen zu einzelnen weiteren Informationssystemen mit Personendaten, die innerhalb des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS), jedoch nicht von der Gruppe Verteidigung, betrieben werden.

Mit der Weiterentwicklung der Armee (WEA) wurden die Strukturen, die Organisation und die Prozesse innerhalb der Armee und der Gruppe Verteidigung grundlegend angepasst. Damit die Aufgaben weiterhin optimal erfüllt werden können, müssen in den Informationssystemen der Gruppe Verteidigung gewisse Personendaten (insb. auch besonders schützenswerte) neu oder in anderer Weise bearbeitet werden können. Dasselbe gilt für Informationssysteme des VBS, die ausserhalb der Gruppe Verteidigung betrieben werden.

Die Rechtsgrundlagen, die das Datenschutzrecht hierfür verlangt (vgl. Art. 17 des Bundesgesetzes vom 19. Juni 1992[2] über den Datenschutz [im Folgenden: aDSG] bzw. Art. 34 des Datenschutzgesetzes vom 25. September 2020[3] [im Folgenden: nDSG], welches das aDSG ablösen wird) fehlen derzeit und müssen geschaffen werden.

1.2 Lösungsvorschlag

Damit man im VBS den datenschutzrechtlichen Anforderungen gerecht wird, sollen die Bestimmungen des MIG zu den bestehenden Informationssystemen wo nötig angepasst und Bestimmungen für neue, benötigte Informationssysteme geschaffen werden.

1.3 Verhältnis zur Legislaturplanung und zur Finanzplanung sowie zu Strategien des Bundesrates

Die Vorlage ist weder in der Botschaft vom 29. Januar 2020[4] zur Legislaturplanung 2019–2023 noch im Bundesbeschluss vom 21. September 2020[5] über die Legislaturplanung 2019–2023 angekündigt. Die vorgeschlagene Änderung der im MIG enthaltenen Rechtsgrundlagen für militärische und andere Informationssysteme des VBS ist

1 SR **510.91**
2 SR **235.1**
3 BBl **2020** 7639
4 BBl **2020** 1777
5 BBl **2020** 8385

jedoch Voraussetzung, damit das VBS und insbesondere die Gruppe Verteidigung und die Armee ihre gesetzlichen Aufgaben optimal wahrnehmen können. Entsprechend trägt sie dazu bei, dass verschiedene Ziele erfüllt und Massnahmen umgesetzt werden können, die im Bundesbeschluss über die Legislaturplanung 2019–2023 genannt werden (etwa das Ziel 15: «Die Schweiz kennt die Bedrohungen ihrer Sicherheit und verfügt über die notwendigen Instrumente, um diesen wirksam entgegenzutreten»[6]). Weiter trägt sie dazu bei, dass sich das vom Bundesrat für das Jahr 2021 gesetzte Ziel erreichen lässt, staatliche Leistungen effizient und möglichst digital zu erbringen.[7] Auswirkungen auf die Finanzplanung sind keine zu erwarten.

1.4 Umsetzungsfragen

Der Bundesrat strebt an, die Änderung des MIG am 1. Februar 2023 in Kraft zu setzen.

Die Änderung des MIG muss durch Ausführungsbestimmungen auf Verordnungsstufe konkretisiert werden. Der Bundesrat und das VBS werden diese Ausführungsbestimmungen rechtzeitig erarbeiten, damit sie gleichzeitig mit der Gesetzesänderung in Kraft treten können.

1.5 Erledigung parlamentarischer Vorstösse

Es werden keine Aufträge von Motionen oder Postulaten erfüllt.

2 Vorverfahren, insbesondere Vernehmlassungsverfahren

2.1 Vorverfahren und Ergebnisse des Vernehmlassungsverfahrens

Vor dem Vernehmlassungsverfahren konnten keine relevanten Auswirkungen der Vorlage etwa auf die Umwelt, die Gesellschaft, die Gesamtwirtschaft, die Gesundheit, die Regionen oder das Ausland festgestellt werden, weshalb keine vertiefte Regulierungsfolgenabschätzung durchgeführt wurde. Auch wurden keine Expertenkommissionen eingesetzt.

Das Vernehmlassungsverfahren dauerte vom 20. Mai 2020 bis zum 11. September 2020.[8] Die Vernehmlassungsteilnehmerinnen und -teilnehmer, die eine inhaltliche Stellungnahme abgaben, befürworteten die Vernehmlassungsvorlage vorbehaltslos oder mit einzelnen Änderungsanträgen. Abgelehnt wurde die Vorlage von niemandem.

6 BBl **2020** 8385, hier 8391
7 BBl **2020** 8385, hier 8386 (Ziel 2); Ziele des Bundesrates 2021, Band I, Ziel 2, S. 10 ff., einsehbar unter www.bk.admin.ch > Dokumentation > Führungsunterstützung > Jahresziele.
8 Die Ergebnisse des Vernehmlassungsverfahrens sind einsehbar unter www.admin.ch > Bundesrecht > Vernehmlassungen > Abgeschlossene Vernehmlassungen > 2020 > VBS.

Anträge, die mehrfach und von zahlreichen Vernehmlassungsteilnehmerinnen und -teilnehmern geltend gemacht wurden, bezogen sich im Wesentlichen auf folgende Aspekte:

- Berücksichtigung der Bedürfnisse der Kantone für eine effiziente und sichere Bewirtschaftung der Personendaten;
- keine Unterdrückung oder Löschung von Daten, welche die Kantone zur Erfüllung ihrer Aufgaben noch benötigen;
- Prüfung einer Erweiterung des Personalinformationssystems der Armee und des Zivilschutzes (PISA) auf den Zivildienst und die Zivildienstleistenden sowie Führung der geleisteten Zivildiensttage durch die Zivildienststellen über das PISA, damit diese Daten dem mit dem PISA verbundenen System Wehrpflichtersatz zur Verfügung stehen, um die Wehrpflichtersatzabgabe erheben und sie bei vollständig geleisteter Dienstpflicht wieder rückerstatten zu können (als Alternative dazu schlug ein Vernehmlassungsteilnehmer vor, eine Schnittstelle von E-ZIVI zu den Systemen der Wehrpflichtersatzabgabe anzustreben);
- Verlängerung der in Artikel 17 Absatz 5 geregelten, in einzelnen Fällen nicht ausreichenden Dauer der Aufbewahrung von gewissen PISA-Daten (von längstens fünf Jahren nach der Entlassung aus der Militär- oder Schutzdienstpflicht auf längstens zehn Jahre);
- Berücksichtigung der Regelungen des Bevölkerungs- und Zivilschutzgesetzes vom 20. Dezember 2019[9] (BZG) (das BZG ist am 1. Januar 2021 in Kraft getreten);
- Berücksichtigung der Regelungen des nDSG, welches das aDSG ablösen wird.

Bei den übrigen Anträgen handelt es sich jeweils um Einzelanträge, die mehrheitlich von bloss einer Vernehmlassungsteilnehmerin oder einem Vernehmlassungsteilnehmer vorgebracht wurden.

Für Einzelheiten zu den Anträgen wird auf den Ergebnisbericht zum Vernehmlassungsverfahren verwiesen.

2.2 Würdigung der Ergebnisse des Vernehmlassungsverfahrens

2.2.1 Übernommene Anträge und weitere Änderungen

Gestützt auf die Anträge, die im Vernehmlassungsverfahren gestellt wurden, wurden gegenüber der Vernehmlassungsvorlage die folgenden wesentlichen materiellen Anpassungen vorgenommen:

- Anpassungen an das nDSG im Wortlaut von Artikel 1 Absatz 1 MIG und durch Einfügung einer Grundlage für die Möglichkeit der Datenbearbeitung durch «Profiling», einschliesslich durch «Profiling mit hohem Risiko», in Artikel 2*b*;

9 SR **520.1**

- Anpassung der Verweise auf das neue BZG in Artikel 15 Absatz 2 Buchstabe a und Artikel 17 Absatz 1 Buchstabe e;
- Eigenständige Nennung der Armee nebst dem VBS im Einleitungssatz von Artikel 1 Absatz 1 zwecks klarerer Abgrenzung (analog der im geltenden Art. 1 Abs. 1 MIG bestehenden Abgrenzung zwischen Armee und Militärverwaltung);
- Die in Artikel 167*l* vorgesehene Aufbewahrungsdauer für Daten des Informationssystems Präventiver Schutz der Armee (IPSA) wurde verkürzt.

Weiter wurde in den Erläuterungen zu den einzelnen Bestimmungen auf verschiedene Anträge hin Folgendes ergänzt:

- Verweise auf das nDSG und das BZG;
- Ergänzung der Begründung für die in Artikel 125 Absatz 2 vorgesehene verlängerte Aufbewahrungsdauer;
- Präzisierung, dass Daten gestützt auf Artikel 167*j* unabhängig von der Art und Weise ihrer Beschaffung bekanntgegeben werden dürfen;
- Präzisierung des in Artikel 179*p* Buchstabe a vorkommenden Begriffs der «künftig möglichen» Geschäftspartnerinnen und Geschäftspartner;
- Ergänzung der Erläuterungen zu Artikel 186 Absatz 3 mit einem Hinweis auf die internationale Zusammenarbeit gemäss Artikel 6 als möglichen Anwendungsfall, in welchem der Bundesrat internationale Abkommen über die grenzüberschreitend erfolgende Bearbeitung von gewissen Personendaten abschliessen kann.

Weiter wurden gegenüber der Vernehmlassungsvorlage und dem Erläuternden Bericht folgende Änderungen vorgenommen, die im Vernehmlassungsverfahren nicht beantragt wurden:

- Artikel 1 Absatz 2 und die zugehörigen Erläuterungen wurden leicht umformuliert, um klarzustellen, dass das MIG weder für die Datenbearbeitung durch den Nachrichtendienst des Bundes noch für die Datenbearbeitung durch den Nachrichtendienst der Armee gilt.
- Gewisse Daten des PISA und des Informationssystems Administration für Dienstleistungen (MIL Office) sollen nicht nur zur Verhinderung von Missbräuchen der Erwerbsersatzordnung, sondern zur Durchführung der Erwerbersatzordnung bearbeitet werden können (vgl. die entsprechenden Änderungen in den Art. 13 Bst. f, 16 Abs. 1 Bst. h, 85 Abs. 2 und 88 Bst. d sowie den zugehörigen Erläuterungen).
- In Artikel 17 Absatz 4^{quater} wurde durch Einfügen des Wortes «längstens» präzisiert, dass die Daten nicht zwingend fünf Jahre aufbewahrt werden müssen.
- In Artikel 140 Buchstaben c und d wurde verdeutlicht, dass nur die Ergebnisse der letzten Kontrolluntersuchung und das Datum der nächsten Kontrolluntersuchung, jedoch keine Daten zu weiter zurückliegenden Kontrolluntersuchungen im Informationssystem Strassenverkehr und Schifffahrt der Armee (FA-SVSAA) enthalten sein müssen.
- In Artikel 143*c* Buchstabe l wurden die im Informationssystem Fliegerische Aus- und Weiterbildung (SPHAIR-Expert) zu bearbeitenden Daten ergänzt.

- Der Zweck des Informationssystems Personensicherheitsprüfung (SIBAD) wurde in Artikel 145 präzisiert.
- In Artikel 147 Absatz 2 Buchstabe c wurde das noch erwähnte, jedoch nicht mehr existente Staatsschutz-Informations-System durch das Informationssystem INDEX NDB ersetzt. Die Erläuterungen wurden entsprechend ergänzt.
- Die Bekanntgabe von Daten des IPSA soll auch an das Bundesamt für Polizei möglich sein (siehe Art. 167*k* Abs. 2 Bst. h).
- Die Bezeichnung und die Abkürzung des Informationssystems Vereins- und Verbandsadministration (VVAdmin) wurden zu Informationssystem Schiesswesen ausser Dienst (SaD) geändert (Art. 179*g*–179*l* und Gliederungstitel vor Art. 179*g*).
- Zudem wurden kleinere sprachliche oder gesetzestechnisch bedingte Anpassungen ohne materielle Auswirkungen vorgenommen (z. B. Änderung des Gliederungstitels vor Art. 168 nur im französischen und italienischen Text; Anpassung des in Art. 146 des Militärgesetzes vom 3. Februar 1995[10] [MG] enthaltenen Verweises auf das MIG, der wegen der Änderung des Erlasstitels des MIG angepasst werden muss).

2.2.2 Nicht übernommene Anträge

Nicht in die Vorlage übernommen wurden folgende Anträge aus den jeweils nachfolgenden genannten Gründen:

- In vereinzelten Anträgen wurde generell die Einhaltung allgemeiner datenschutzrechtlicher Prinzipien und Grundsätze sowie von Bestimmungen des aDSG verlangt. Sofern das MIG nichts anderes regelt, gelten diese aufgrund des Verweises auf das aDSG in Artikel 1 Absatz 3 MIG schon jetzt für sämtliche Informationssysteme des MIG. Diesbezügliche Änderungen oder Konkretisierungen im MIG sind nicht nötig und wurden nicht vorgenommen. Anzumerken bleibt, dass die Bestimmungen des MIG für jedes einzelne Informationssystem bereits hinreichend detailliert regeln, welche Daten zu welchen Zwecken und wie lange bearbeitet sowie bei wem beschafft und wem bekanntgegeben werden dürfen. Konkretisiert wird dies überdies in den Bearbeitungsreglementen (vgl. Art. 36 Abs. 4 aDSG i.V.m. Art. 21 der Verordnung vom 14. Juni 1993[11] zum Bundesgesetz über den Datenschutz [VDSG]) bzw. künftig in den Verzeichnissen der Bearbeitungstätigkeiten (vgl. Art. 12 nDSG), die zu den einzelnen Informationssystemen jeweils bestehen. Damit wird den allgemeinen datenschutzrechtlichen Prinzipien nachgelebt, insbesondere demjenigen, wonach die Datenbearbeitung nur rechtmässig und verhältnismässig sowie zu einem bestimmten Zweck erfolgen darf (Art. 4 Abs. 1–3 aDSG bzw. Art. 6 Abs. 1–3 nDSG).
- Ob Daten von Amtes wegen oder auf Anfrage von Interessierten hin bekanntgegeben werden, wurde in den jeweiligen Bestimmungen nicht wie beantragt präzi-

10 SR **510.10**
11 SR **235.11**

siert. Ist eine Datenbekanntgabe vorgesehen und wird nichts weiter erwähnt, bedeutet dies, dass die Bekanntgabe von Amtes wegen und auf Gesuch hin möglich ist und auch sein soll, um den mit der Bekanntgabe verfolgten Zweck und die damit verbundenen Aufgaben möglichst optimal erfüllen zu können.

- Im Erlasstitel wurde «Bundesgesetz über die militärischen und anderen Informationssysteme im VBS» nicht wie beantragt zu «Bundesgesetz über die militärischen Informationssysteme und über die Informationssysteme im VBS» geändert. Die militärischen Informationssysteme, die im MIG geregelt sind, werden von der Gruppe Verteidigung bzw. von den ihr untergeordneten Verwaltungseinheiten bzw. Ämtern, das heisst von der Militärverwaltung, betrieben und insbesondere der Armee zur Verfügung gestellt. Die Militärverwaltung ist Teil des VBS. Insofern handelt es sich bei den militärischen Informationssystemen um solche, die «im VBS» betrieben werden. Eine Unterstellung der Armee unter das VBS lässt sich dem neuen Erlasstitel nicht entnehmen.
- In Artikel 8 wurde keine Regelung betreffend die Dauer der Archivierung bzw. die Löschung von Daten aus den Archiven aufgenommen. Die Archivierung wird nicht im MIG geregelt, sondern richtet sich nach dem Archivierungsgesetz vom 26. Juni 1998[12] (BGA). Ein bloss deklaratorischer Verweis auf das BGA in Artikel 8 ist unnötig.
- Die Erläuterungen zu Artikel 8 wurden nicht um eine Anmerkung ergänzt, wonach vor der Löschung von Daten die Bedürfnisse jener Kantone unbedingt zu berücksichtigen seien, die auf diese Daten angewiesen sind. Bei Artikel 8 handelt es sich um eine allgemeine Bestimmung, die für sämtliche im MIG geregelten Informationssysteme gilt. Sie ist Ausfluss des Verhältnismässigkeitsprinzips (vgl. auch Art. 4 Abs. 2 aDSG bzw. Art. 6 Abs. 2 und 4 nDSG) und besagt in genereller Weise, dass nicht mehr benötigte Daten gelöscht werden müssen. Ob überhaupt und für wie lange Daten eines bestimmten Informationssystems den Kantonen zu bestimmten Bearbeitungszwecken bekanntgegeben werden dürfen und sollen (und insofern zugunsten der Kantone noch benötigt werden), bestimmt sich dagegen nicht nach Artikel 8. Dies regeln die besonderen Bestimmungen des MIG zu den einzelnen Informationssystemen (siehe insb. die Bestimmungen zum Zweck der Datenbearbeitung, zur Datenbekanntgabe und zur Datenaufbewahrung).
- Es wurde keine Erweiterung des Personalinformationssystems der Armee und des Zivilschutzes (PISA) auf den Zivildienst und die Zivildienstleistenden vorgesehen. Die Vorbereitung, Durchführung und Verwaltung von Zivildiensteinsätzen erfolgt über das hierfür eigens bestehende Informationssystem E-ZIVI (vgl. Art. 80 des Zivildienstgesetzes vom 6. Oktober 1995[13] [ZDG] i.V.m. der Verordnung vom 20. August 2014[14] über das Informationssystem des Zivildienstes). Diese gesetzlich vorgesehene Datenhaltung erweist sich in der Praxis als sinnvoll, bestehen doch unterschiedliche Bedürfnisse bei der Vorbereitung, Verwaltung und Abrechnung von Dienstleistungen im Bereich des Zivildienstes einerseits so-

12 SR **152.1**
13 SR **824.0**
14 SR **824.095**

wie in den Bereichen der Armee und des Zivilschutzes andererseits. Die Entwicklung und der Betrieb des automatisierten Informationssystems E-ZIVI obliegt dem im Eidgenössischen Departement für Wirtschaft, Bildung und Forschung (WBF) angesiedelten Bundesamt für Zivildienst (ZIVI). Was die von den Kantonen vorgebrachten Probleme im Zusammenhang mit der Erhebung der Wehrpflichtersatzabgabe bei Zivildienstpflichtigen und deren Rückerstattung bei vollständig geleisteter (Zivil-)Dienstpflicht anbelangt, wird auf die im Zivildienstrecht vorgesehene Möglichkeit verwiesen, die Behörden des Wehrpflichtersatzes für ersatzrechtliche Handlungen direkt (online) an das E-ZIVI anzuschliessen (Art. 80 Abs. 2 Bst. e ZDG). Die entsprechende Umsetzung erfolgt durch das hierfür zuständige ZIVI. Diese Thematik ist indessen nicht Teil dieser Vorlage, da sie nicht unter den Regelungsgegenstand des MIG fällt: Dieser beschränkt sich in der neuen Fassung (vgl. Art. 1 Abs. 1 E-MIG) nämlich auf die Datenbearbeitung in Informationssystemen des VBS.

– Dass in den Ausführungsbestimmungen zum MIG gestützt auf Artikel 186 Absatz 1 Buchstabe a MIG das Kommando Ausbildung als Inhaberin der Datensammlung PISA und für den Datenschutz verantwortliches Bundesorgan bezeichnet wird (vgl. Art. 2*a* i.V.m. Anhang 1 der Verordnung vom 16. Dezember 2009[15] über die militärischen Informationssysteme [MIV]), stellt keine Inkohärenz dar und erfordert keine Anpassungen in der Vorlage. Denn das PISA, das auch Daten von Zivilschutzleistenden enthält, wird, wie in Artikel 13 MIG vorgesehen, von der Gruppe Verteidigung und nicht etwa von den für den Zivilschutz zuständigen Stellen und Behörden betrieben. Der Gruppe Verteidigung kommt somit die Gesamtverantwortung für das PISA und den Schutz jener Daten zu, die darin bearbeitet werden. Wie bei den anderen Informationssystemen, die gemäss Gesetz von der Gruppe Verteidigung betrieben werden, definiert der Bundesrat die Verwaltungseinheit, die innerhalb der Gruppe Verteidigung für den Datenschutz zuständig ist (vorliegend: Kommando Ausbildung). Die Gruppe Verteidigung bzw. das Kommando Ausbildung ist für den Schutz der PISA-Daten (gesamt-)verantwortlich. Die Stellen und Behörden des Zivilschutzes haben die Kontrolle über die Schutzdienstpflichtigen im PISA zu führen (vgl. Art. 47 Abs. 1 BZG) und die dafür benötigten Daten im PISA zu erfassen. Damit sie diese Aufgaben wahrnehmen können, erteilt ihnen die Gruppe Verteidigung mittels Abrufverfahren Zugriff auf die PISA-Daten (vgl. Art. 16 Abs. 1 Bst. f MIG).

– Die Meldepflichtigen wurden im Einleitungssatz von Artikel 14 Absatz 1 nicht zusätzlich erwähnt. Artikel 14 Absatz 1 regelt lediglich die im PISA enthaltenen Daten von Personen, die einer im Zusammenhang mit der Armee stehenden Personengruppe angehören. Die im PISA enthaltenen Daten von Zivildienst- oder Schutzdienstpflichtigen werden in Artikel 14 Absätze 2 und 3 geregelt. Für die Armee gehören zu den meldepflichtigen Personen die Stellungspflichtigen und die Militärdienstpflichtigen (vgl. Art. 27 Abs. 1 MG). Da die Stellungspflichtigen und Militärdienstpflichtigen in Artikel 14 Absatz 1 bereits genannt sind, bedarf es der beantragten Nennung der Meldepflichtigen als weiterer Personengruppe nicht.

15 SR **510.911**

- Der geläufigere Begriff der Zivildienstpflichtigen wurde im Einleitungssatz von Artikel 14 Absatz 2 nicht mit «Militärdienstpflichtigen, die den freiwilligen Ersatzdienst leisten» ersetzt. Denn das ZDG verwendet durchwegs ebenfalls die Begriffe des Zivildienstes und der Zivildienstpflicht bzw. der zivildienstpflichtigen Person. Derjenige des «Ersatzdienstes» findet sich im ZDG hingegen bloss im Erlasstitel und in Artikel 1. Zudem führt Artikel 1 ZDG für den Begriff des zivilen Ersatzdienstes mittels Klammerdefinition auch die Kurzform «Zivildienst» ein. Der Einheitlichkeit halber ist daher die bestehende Begrifflichkeit in Artikel 14 Absatz 2 MIG beizubehalten.
- Die in Artikel 17 Absatz 5 vorgesehene Datenaufbewahrungsdauer von längstens fünf Jahren wurde nicht auf zehn Jahre verlängert. Auch wurde der Beginn der maximal fünfjährigen Aufbewahrungsdauer nicht zusätzlich an die vollständige Leistung der Wehrpflichtersatzabgabe geknüpft, die allenfalls auch erst nach der Entlassung aus der Militärdienst- oder Schutzdienstpflicht erfolgen kann. Überdies wurde in Artikel 17 Absatz 3 nicht zusätzlich erwähnt, dass eine Aufbewahrung der Daten in gewissen Fällen bis zum Jahr möglich sei, in dem die betreffende Person das 40. Altersjahr erreicht. Da das PISA primär die militärische und zivilschutzdienstliche Kontrollführung und nicht die Erhebung und Kontrolle der Wehrpflichtersatzabgabe bezweckt (vgl. Art. 13 MIG), rechtfertigen Probleme im Zusammenhang mit der Wehrpflichtersatzabgabe keine Verlängerung der Aufbewahrungsdauer. Eine solche Verlängerung würde den datenschutzrechtlichen Verhältnismässigkeitsgrundsatz verletzen, nach dem Daten nur so lange wie für die Zweckerfüllung nötig bearbeitet werden dürfen. Würde man die Aufbewahrungsdauer um fünf Jahre verlängern, so müssten bei der automatisierten Pflege und Aktualisierung der Daten aus den Gemeinderegistern zudem weitere fünf Jahrgänge verarbeitet werden. Dies entspricht rund 71 500 Angehörigen der Armee und 35 000 Angehörigen des Zivilschutzes. Bei einer solchen Ausdehnung müsste das automatisierte Pflege- und Aktualisierungssystem ausgebaut werden, da es seine Grenzkapazität bereits erreicht hat und sonst kollabieren würde. Dies würde zu Mehrkosten in noch nicht definiertem Umfang führen. Die Kosten stünden in keinem vernünftigen Verhältnis zum erreichten Nutzen. Schliesslich wäre es praktisch auch nicht umsetzbar, wenn der Beginn der maximalen Aufbewahrungsdauer an die vollständige Leistung der Wehrpflichtersatzabgabe angeknüpft würde. Dieser Zeitpunkt wird nämlich im PISA nicht erfasst und ist daher der Gruppe Verteidigung nicht bekannt.
- Unbegründet ist die von einem Vernehmlassungsteilnehmer geäusserte Befürchtung, wonach die vorgesehene Aufhebung von Artikel 47 Absatz 1 den Datenschutz weniger garantiere. Beim Informationssystem Flugmedizin (MEDIS LW) handelt es sich um ein eigenständiges, von anderen Informationssystemen abgesondertes Informationssystem mit eigenen Daten sowie spezifisch geregelten Zugriffsberechtigungen. Die Daten werden zudem im MEDIS LW nur so lange aufbewahrt, wie dies in Artikel 47 gesetzlich vorgesehen ist. Für die spätere Archivierung der Daten ist nicht die Gruppe Verteidigung (bzw. das Fliegerärztliche Institut) zuständig, sondern das Bundesarchiv. Wurden die Daten dem Bundesarchiv zur Archivierung angeboten, so werden sie bei der Gruppe Verteidigung anschliessend vernichtet (vgl. Art. 8).

- In Artikel 56 nicht näher definiert wurden die Dokumente, die unter den Begriff «persönliche Dokumente, die für die Beurteilung einer sozialen Beratung und Betreuung notwendig sind» fallen. Der Sozialdienst der Armee verfolgt einen umfassenden Ansatz bei seiner sozialen Beratung und Betreuung, die inhaltlich entsprechend vielgestaltig sein kann. Daher kann es sich auch bei den persönlichen Dokumenten, die für die Beurteilung einer konkreten sozialen Beratung und Betreuung notwendig sind, um alle möglichen Dokumente handeln. Entsprechend ist der Begriff der persönlichen Dokumente in Artikel 56 unbestimmt zu nennen. Würden die für die Beurteilung einer sozialen Beratung und Betreuung notwendigen Dokumente, die im Informationssystem bearbeitet werden dürfen, einschränkender definiert, so käme dies einer Einschränkung der angebotenen Palette möglicher sozialer Beratungs- und Betreuungsmassnahmen gleich. Diese Massnahmen könnten eventuell nicht mehr hinreichend beurteilt und gewährt werden, wenn benötigte Dokumente fehlen. Dies wäre letztlich nachteilig für die Personen, die von der sozialen Beratung und Betreuung profitieren möchten. Auch bleibt zu beachten, dass die Inanspruchnahme der sozialen Beratung und Betreuung wie auch die Einreichung persönlicher Dokumente durch die betreffende Person stets freiwillig sind. Es steht der betreffenden Person frei, persönliche Dokumente nicht einzureichen oder eine soziale Beratungs- oder Betreuungsmassnahme nicht in Anspruch zu nehmen.
- Eine Verkürzung der insbesondere in den Artikeln 125 Absatz 2, 131, 143 Absätze 1 und 2, 173 und 179*r* Absatz 2 je vorgesehenen Datenaufbewahrungsdauer konnte nicht in Betracht gezogen werden. Wie dies teilweise in den zugehörigen Erläuterungen erwähnt wird, müssen die Daten für eine zweckmässige Erfüllung der jeweiligen Verwaltungs- und Kontrollaufgaben während der jeweils vorgesehenen längeren Aufbewahrungsdauer verfügbar sein.
- Es wurde auf Erläuterungen verzichtet, wie die Datensicherheit in den einzelnen Informationssystemen (z. B. JORASYS) gewährleistet werden kann. Diese Frage ist nicht spezifisch für jedes einzelne Informationssystem im MIG zu regeln. Vielmehr kann auf die einschlägigen allgemeinen Bestimmungen des aDSG verwiesen werden, die auch für die im MIG geregelten Informationssysteme grundsätzlich anwendbar sind (vgl. Art. 1 Abs. 3 MIG). Für die Gewährleistung der Datensicherheit verantwortlich ist die jeweilige Inhaberin des Informationssystems und der Datensammlung (vgl. Art. 16 Abs. 1 aDSG i.V.m. Art. 7 aDSG und Art. 20 ff. VDSG; ferner Art. 10*a* Abs. 2 aDSG i.V.m. Art. 22 VDSG insb. auch mit Bezug auf die Datenbearbeitung durch beigezogene externe Leistungserbringerinnen und Leistungserbringer gemäss Art. 7 Abs. 2 E-MIG; im nDSG finden sich die entsprechenden einschlägigen Bestimmungen in Art. 7 i.V.m. Art. 5 Bst. j, Art. 8 i.V.m. Art. 20 ff. VDSG und Art. 9 Abs. 2 i.V.m. Art. 22 VDSG). Die Inhaberin hat durch angemessene technische und organisatorische Massnahmen Personendaten gegen unbefugtes Bearbeiten zu schützen (Art. 7 Abs. 1 aDSG bzw. Art. 8 Abs. 1 und 2 nDSG). Auch ist über die Bearbeitungstätigkeiten ein Bearbeitungsreglement zu führen, in dem die technischen und organisatorischen Massnahmen zur Gewährleistung der Datensicherheit allgemein zu beschreiben sind (vgl. Art. 21 Abs. 2 VDSG; siehe zudem Art. 12 Abs. 2 Bst. f nDSG, der dies zum Inhalt der künftig zu führenden Verzeichnisse der Bearbei-

tungstätigkeiten zählt). Welche Massnahmen im Einzelnen getroffen werden müssen, ist für jeden konkreten Bearbeitungsfall zu beurteilen und festzulegen – unter Berücksichtigung der damit verbundenen Risiken.

– Einzelne Änderungsanträge zum IPSA wurden nicht übernommen. Keine Option ist die einmal verlangte gänzliche Streichung der Bestimmungen zum IPSA. Denn dieses Informationssystem, das für die Aufgabenerfüllung des Dienstes für präventiven Schutz der Armee (DPSA) erforderlich ist, braucht eine rechtliche Grundlage, mit der die Bearbeitung der benötigten Personendaten legitimiert werden kann. Unbegründet, da unzutreffend, ist die geäusserte Annahme bzw. Befürchtung, dass Daten ausländischer Nachrichtendienste vom Personellen der Armee ohne weitere Prüfung und Verifikation etwa für Laufbahnbeurteilungen des Militärkaders herbeigezogen würden (solche Beurteilungen und die [Über-]Prüfung der Entscheidgrundlagen laufen nach bindend festgelegten Prozessen ab). Auf die Bearbeitung der in Artikel 167*i* Buchstabe e genannten politischen und ideologischen Ausrichtung sollte nicht verzichtet werden, da sich daraus Hinweise auf einen für die Armee bedrohlichen Zusammenhang mit Terrorismus, gewalttätigem Extremismus (z. B. ausgehend von radikalen, extremistischen religiösen Gruppierungen) oder verbotenem Nachrichtendienst ergeben können. Zum Verhältnis und zur Zusammenarbeit zwischen dem DPSA und dem Nachrichtendienst des Bundes (NDB) bedarf es in den Bestimmungen des MIG und in den zugehörigen Erläuterungen keiner Klärung, da dies nicht zum Regelungsgegenstand des MIG gehört, das einzig die Bearbeitung von Personendaten in Informationssystemen des VBS regelt. Stattdessen reicht diesbezüglich ein Verweis auf die einschlägigen Bestimmungen im Nachrichtendienstgesetz vom 25. September 2015[16] (NDG; siehe insb. die Art. 11, 19, 20 und 60) sowie auf Artikel 100 Absatz 1 Buchstabe a und Absatz 4 Buchstabe b MG, ferner zudem auf die zugehörigen Ausführungsbestimmungen des Bundesrates (vgl. nur Art. 1 und 4 sowie Anhang 3 Ziff. 10.3 der Nachrichtendienstverordnung vom 16. August 2017[17] [NDV] sowie Art. 3 der Verordnung vom 21. November 2018[18] über die Militärische Sicherheit [VMS]). Die Zusammenarbeit des DPSA mit anderen Partnern wie in- und ausländischen Nachrichtendiensten wird vorgängig dem Bundesrat im Rahmen der gemeinsamen Partnerdienstpolitik des Nachrichtendienstes der Armee (NDA) und des NDB (vgl. Art. 7 und 8 NDV) jährlich beantragt und vom Bundesrat genehmigt.

3 Grundzüge der Vorlage

Die Vorlage sieht vor, die Bestimmungen des MIG über mehrere bestehende Informationssysteme anzupassen sowie Bestimmungen über neue Informationssysteme in das MIG aufzunehmen. Diese Änderungen betreffen insbesondere folgende Regelungsgegenstände und Informationssysteme:

16 SR **121**
17 SR **121.1**
18 SR **513.61**

- die Ausdehnung des Gegenstands und Geltungsbereichs des MIG unter anderem auf Informationssysteme des VBS, einschliesslich der entsprechenden Änderung des Erlasstitels sowie weiterer, dadurch notwendiger Änderungen in anderen Bestimmungen;
- die Schaffung einer Rechtsgrundlage für die Verwendung und Bearbeitung der AHV-Nummer 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 im Bereich der Informations- und Kommunikationstechnik (IKT) beigezogene Leistungserbringerinnen und 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-Aufklärungsdetachement [EAAD], Informationssystem Militärische Fahrberechtigungen [MIFA]);
- die Präzisierung der Rechtsgrundlage für die Bearbeitung von Personendaten im Informationssystem Schadenzentrum VBS (SCHAWE);
- die Schaffung einer Rechtsgrundlage, damit die in den Informationssystemen oder beim Einsatz von Überwachungsmitteln bearbeiteten Personendaten bei weiteren Stellen, Personen oder Informationssystemen beschafft oder an diese bekanntgegeben oder zu neuen Zwecken bearbeitet werden dürfen;
- die Nennung der Gruppe Verteidigung als Betreiberin diverser Informationssysteme (PISA, Informationssysteme Patientenerfassung [ISPE], 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], SCHAWE, Strategisches Informationssystem Logistik [SISLOG], VVAdmin);
- die Schaffung einer Rechtsgrundlage für die Verwendung bestimmter Daten des MIL Office zur Durchführung der Erwerbsersatzordnung 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. die Neuregelung (MEDIS LW, JORASYS) der Aufbewahrungsdauer von Personendaten;

- die Ermöglichung des durch Abrufverfahren oder automatisiert über eine Schnittstelle erfolgenden Datenzugriffs (SIBAD, JORASYS);
- die Neuaufnahme 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, gesetzestechnisch bedingte oder sprachliche Änderungen (allgemeine Bestimmungen, PISA, Medizinisches Informationssystem der Armee [MEDISA], MEDIS LW, EAAD, ISB, Informationssystem Personal Verteidigung [IPV], IES-KSD, MIL Office, Informationssystem Kompetenzmanagement [ISKM], Führungsinformationssystem Heer [FIS HE], Führungsinformationssystem Soldat [IMESS], MIFA, SIBAD, JORASYS, SCHAWE, SISLOG, Informationssystem integrierte Ressourcenbewirtschaftung [PSN]).

4 Erläuterungen zu einzelnen Artikeln

4.1 Bundesgesetz über die militärischen Informationssysteme (MIG)

Erlasstitel

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

Ingress

Zusätzlich zu den bisher im Ingress genannten Bestimmungen (Art. 40 Abs. 2 und Art. 60 Abs. 1 der Bundesverfassung[19], BV), welche die Rechtsgrundlage für die Regelung der militärischen Informationssysteme bilden, ist als weitere Rechtsgrundlage für die im MIG geregelten nicht militärischen Informationssysteme des VBS (mangels einer expliziten Kompetenzdelegation an den Bund) praxisgemäss der Artikel 173 Absatz 2 BV zu ergänzen.

19 SR **101**

Ersatz eines Ausdrucks

Im ganzen Erlass wird der bisher verwendete Ausdruck «AHV-Versichertennummer» durch den im allgemeinen Sprachgebrauch üblicheren und kürzeren Ausdruck «AHV-Nummer» ersetzt, der sich auch im übrigen Bundesrecht durchsetzt.

Art. 1 Abs. 1 Einleitungssatz und Bst. b–d sowie Abs. 2 und 3

Der zu eng gefasste Geltungsbereich ist derart zu erweitern, dass nicht nur militärische Informationssysteme, sondern auch bereits heute im MIG geregelte nicht militärische Informationssysteme, die das VBS betreibt, erfasst werden (vgl. Art. 1 Abs. 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 andere Aufgaben des 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 und c auch die entsprechenden Personen des Zivilschutzes und in Buchstabe d auch Dritte, die Aufgaben für das Zivilschutzwesen erfüllen, zu nennen sind. Artikel 1 Absatz 1 Buchstabe b ist überdies geschlechtergerecht zu formulieren.

Im Einleitungssatz von Artikel 1 Absatz 1 ist der Klarheit halber zu präzisieren, dass die Bearbeitung von Personendaten sowohl natürlicher wie auch juristischer Personen unter den Geltungsbereich des MIG fällt. Diese Präzisierung ist auch kompatibel mit dem nDSG. Das nDSG wird künftig nur noch für die Bearbeitung von Personendaten natürlicher Personen gelten (vgl. Art. 2 Abs. 1 nDSG), und entsprechend wird die in Artikel 5 Buchstabe a nDSG enthaltene Begriffsdefinition unter Personendaten nur noch solche natürlicher Personen verstehen. Die Bestimmungen des MIG zu den einzelnen Informationssystemen sehen demgegenüber teilweise auch die Bearbeitung von Personendaten juristischer Personen vor. Dem MIG liegt somit ein anderes, weiteres Verständnis des Begriffs Personendaten zugrunde als dem nDSG. Indem dies in Artikel 1 Absatz 1 MIG zum Ausdruck kommt, kann schon jetzt vermieden werden, dass gestützt auf Artikel 1 Absatz 3 MIG das engere Begriffsverständnis des nDSG auch im Bereich des MIG für anwendbar erklärt wird. Denn regelt das MIG etwas besonders, geht dies dem nDSG vor (Art. 1 Abs. 3 MIG).

Weiter ist im Einleitungssatz von Artikel 1 Absatz 1 der nicht mehr erforderliche Begriff der «Persönlichkeitsprofile» zu streichen. Dieser Begriff ist vom Wort «Personendaten» bereits mit umfasst und im nDSG nicht mehr enthalten. Stattdessen ist eine Regelung für das im nDSG ebenfalls vorkommende «Profiling» in Artikel 2*b* vorgesehen. Überdies soll der Einleitungssatz von Artikel 1 Absatz 1 generell die Bearbeitung von (allen) «Personendaten» als Regelungsgegenstand des MIG bezeichnen und insbesondere nicht nur diejenige von besonders schützenswerten Personendaten. Denn das MIG enthält auch Bestimmungen, die sich auf die Bearbeitung von Personendaten beziehen, die nicht besonders schützenswert sind.

Damit die nötigen Anpassungen im Einleitungssatz von Artikel 1 Absatz 1 mit dem Inkrafttreten des nDSG, das noch eine anderslautende Formulierung vorsah, nicht wieder rückgängig gemacht werden, ist in der vorliegenden Änderung des MIG die erforderliche Koordinationsbestimmung vorzusehen (siehe Ziff. 5.1).

Artikel 1 Absatz 2 ist dahingehend zu präzisieren, dass die (andernorts geregelte) Datenbearbeitung durch die Nachrichtendienste des Bundes und der Armee vom Geltungsbereich ausgenommen ist, jedoch nicht gänzlich jede Bearbeitung von Daten, welche die Nachrichtendienste oder etwa deren Mitarbeiterinnen und Mitarbeiter betreffen.

In Artikel 1 Absatz 3 ist die Abkürzung des aDSG einzuführen, die später wiederverwendet wird (siehe Art. 6 Bst. b und Art. 186 Abs. 3). Damit die Abkürzung auch mit dem Inkrafttreten des nDSG beibehalten bleibt, ist in der vorliegenden Änderung des MIG die erforderliche Koordinationsbestimmung vorzusehen (siehe Ziff. 5.1).

Art. 2 Abs. 1 Einleitungssatz und Bst. a

Aufgrund des zu erweiternden Geltungsbereichs des MIG (vgl. Erläuterungen zu Art. 1 Abs. 1 Einleitungssatz) gelten dessen allgemeine Bestimmungen, insbesondere Artikel 2 (Grundsätze der Datenbearbeitung), auch für die im MIG geregelten 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 50*e* Absatz 1 des Bundesgesetzes vom 20. Dezember 1946[20] über die Alters- und Hinterlassenenversicherung erforderliche rechtliche Grundlage für die Verwendung der AHV-Nummer 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]) übergreifend für das gesamte VBS betrieben werden, ist die Verwendung der AHV-Nummer als Personenidentifikator auch im nicht militärischen Bereich des VBS für eine effiziente Verwaltungstätigkeit und Aufgabenerfüllung unerlässlich.

Artikel 2 Absatz 1 Buchstabe a ist aufzuheben, da bereits die gemäss Artikel 1 Absatz 3 MIG anwendbaren Artikel 17 und 19 Absatz 3 aDSG (bzw. künftig Art. 34 nDSG) regeln, dass die Bearbeitung von Personendaten eine rechtliche Grundlage erfordert und wann diese in einem Gesetz im formellen Sinn enthalten sein muss. Für die Bearbeitung von nicht besonders schützenswerten Personendaten bedarf es grundsätzlich – sofern sich aus ihnen nicht etwa ein Persönlichkeitsprofil ergibt – keiner Grundlage in einem Gesetz im formellen Sinn. Es genügt vielmehr eine Bestimmung in einer Verordnung des Bundesrates (vgl. Art. 17 und 19 Absatz 3 aDSG bzw. Art. 34 Abs. 1 und 2 nDSG, Art. 186 Abs. 1 Bst. b MIG).

20 SR **831.10**

Art. 2b Profiling

Die Möglichkeit, Daten zu bestimmten Bearbeitungszwecken auch durch «Profiling», einschliesslich durch «Profiling mit hohem Risiko», bearbeiten zu dürfen, ist in Artikel 2*b* vorzusehen. Diese beiden Bearbeitungsarten sind auch im neuen DSG[21] geregelt. Als «Profiling» gilt «jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen» (Art. 5 Bst. f nDSG). Bei einem «Profiling mit hohem Risiko» handelt es sich um ein «Profiling, das ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt, indem es zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt» (Art. 5 Bst. g nDSG). Mit der neuen Regelung in Artikel 2*b* wird die künftig nach Artikel 34 Absatz 2 Buchstabe b nDSG für das «Profiling» und das «Profiling mit hohem Risiko» erforderliche Grundlage in einem Gesetz im formellen Sinn geschaffen. Sie sieht die Bearbeitung bestimmter persönlicher Aspekte einer natürlichen Person durch «Profiling», einschliesslich durch «Profiling mit hohem Risiko», zu bestimmten Bearbeitungszwecken wie folgt vor:

Analyse, Bewertung, Beurteilung oder Vorhersage folgender **persönlicher Aspekte**:	Zu den **Bearbeitungszwecken** nach folgenden Bestimmungen des MIG:					
	Artikel 13 (PISA)	Artikel 127 (LMS VBS)	Artikel 143*b* (SPHAIR-Expert)	Artikel 143*h* (Informationssystem Führungsausbildung [ISFA])	Artikel 145 (SIBAD)	Weitere
Tauglichkeit und Fähigkeit für die Leistung von Militär- und Schutzdienst, einschliesslich tauglichkeits- und fähigkeitsrelevanter Voraussetzungen	x (Bst. b–d)					
Eignung zur Ausübung bestimmter Funktionen, Tätigkeiten und Arbeiten, einschliesslich eignungsrelevanter Voraussetzungen	x (Bst. b–d)		x (Bst. d und e)			
Leistungsprofil und Leistungsfähigkeit, insbesondere in den Bereichen Gesundheit, Körper, Intelligenz, Persönlichkeit, Psyche, Sozialverhalten und Verkehrsverhalten	x (Bst. b–d)		x (Bst. d und e)			

21 BBl **2020** 7639

Analyse, Bewertung, Beurteilung oder Vorhersage folgender **persönlicher Aspekte**:	Zu den **Bearbeitungszwecken** nach folgenden Bestimmungen des MIG:					
	Artikel 13 (PISA)	Artikel 127 (LMS VBS)	Artikel 143*b* (SPHAIR-Expert)	Artikel 143*h* (Informationssystem Führungsausbildung [ISFA])	Artikel 145 (SIBAD)	Weitere
Kenntnisse, Kompetenzen, Fähigkeiten und erbrachte Leistungen	x (Bst. b–d)	x (Bst. d und e)	x (Bst. d und e)	x		
Lernverhalten und -fortschritt		x (Bst. a–c)				
Kaderpotenzial und Entwicklungsmöglichkeiten	x (Bst. b–d und m)					
Persönliche Interessen hinsichtlich des Militär- und Schutzdienstes, der Anstellung, der Ausbildung sowie der Weiterentwicklung	x (Bst. b–d und m)	x (Bst. b)	x (Bst. a, d und e)			
Sicherheitsrisiko sowie Gefährdungs- und Missbrauchspotenzial bezüglich der persönlichen Waffe	x (Bst. l)				x	
Weitere persönliche Aspekte						x (mit Einwilligung der betreffenden Person)

Aufgrund von Artikel 2*b* sollen – mit Ausnahme der Datenbearbeitung im Informationssystem SPHAIR-Expert nach Artikel 2*b* Buchstabe g (vgl. Erläuterungen zu Art. 143*c* Bst. l) – keine Datenbearbeitungen vorgenommen werden, die nicht bereits heute von den verantwortlichen Organen (z. B. anlässlich der Rekrutierung) durchgeführt werden. Insofern stellt Artikel 2*b* bloss eine Anpassung der Rechtsgrundlagen an die Anforderungen des nDSG an die Normstufe dar.

Art. 3

Aufgrund des zu erweiternden Geltungsbereichs des MIG (vgl. Erläuterungen zu Art. 1 Abs. 1 Einleitungssatz) sind insbesondere für die nicht militärischen Informationssysteme auch weitere Leistungserbringer neben der Führungsunterstützungsbasis der Armee denkbar. Artikel 3 (Betrieb der Informationssysteme) ist daher aufzuheben.

Der technische Betreiber eines jeweiligen Informationssystems kann etwa im Bearbeitungsreglement (vgl. Art. 36 Abs. 4 aDSG i.V.m. Art. 21 VDSG) bzw. künftig im Verzeichnis der Bearbeitungstätigkeiten nach Artikel 12 nDSG festgelegt werden.

Art. 4 Abs. 1

Aufgrund des zu erweiternden Geltungsbereichs des MIG (vgl. Erläuterungen zu Art. 1 Abs. 1 Einleitungssatz) sollen mit der Änderung von Artikel 4 Absatz 1 auch nicht militärische Informationssysteme des VBS in den in Artikel 4 geregelten Verbund von Informationssystemen eingebunden werden können. Ausserdem soll die in den Ausführungsbestimmungen zum MIG (vgl. Art. 2 Abs. 2 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 auf Gesetzesstufe verankert werden.

Art. 6 Datenbearbeitung im Rahmen der internationalen Zusammenarbeit

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 (so der Geltungsbereich gemäss bisherigem Art. 1 Abs. 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 aDSG angebracht, wo jeweils bloss für die Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen eine Regelung in einem Gesetz im formellen Sinn verlangt wird. Auch das nDSG wird für die Bearbeitung von nicht besonders schützenswerten Personendaten grundsätzlich keine Grundlage in einem Gesetz im formellen Sinn verlangen (vgl. Art. 34 Abs. 2 nDSG).

Art. 7 Abs. 2 erster Satz

Bundesinterne IKT-Leistungserbringerinnen und -Leistungserbringer sind aus Kosten- und Effizienzgründen auf die Zusammenarbeit mit IKT-Dienstleisterinnen und -Dienstleistern ausserhalb der eigenen Verwaltungseinheit oder ausserhalb der Bundesverwaltung angewiesen. Dies kann mit sich bringen, dass diesen IKT-Dienstleisterinnen und -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 Unterbruchszeit 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-Leistungserbringerinnen und -Leistungserbringer zählen.

Art. 8 Aufbewahrung, Archivierung und Vernichtung der Daten

Artikel 8 soll einfacher und entsprechend dem zeitlich-logischen Ablauf der Datenhaltung und -archivierung formuliert werden. Anders als bisher soll daher nicht zuerst von der Löschung nicht benötigter Daten und erst danach von deren Anbieten zur Archivierung die Rede sein. 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 (Einschränkungen der Datenbearbeitung) aufgehoben werden kann.

Damit die Aufhebung von Artikel 11 mit dem Inkrafttreten des nDSG, das noch eine Änderung von Artikel 11 vorsah, nicht wieder rückgängig gemacht wird, ist in der vorliegenden Änderung des MIG die erforderliche Koordinationsbestimmung vorzusehen (siehe Ziff. 5.1).

Art. 13 Bst. f und n–p; Art. 14 Abs. 1 Bst. a^{bis}, c^{bis} und n, Abs. 2 Einleitungssatz und Abs. 4; Art. 15 Abs. 1 Einleitungssatz, Abs. 2 Bst. a und Abs. 4; Art. 16 Abs. 1 Einleitungssatz, Bst. b^{bis}, h und i sowie Abs. 1ter; Art. 17 Abs. 1 Bst. e und Abs. 4ter, 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. Art. 18 ff. MIG) und der FallDok PPD (vgl. Art. 36 ff. MIG) – in das PISA.

Für die Integration des ITR sind die PISA-Bestimmungen wie folgt anzupassen:

- Artikel 14 Absatz 1 Buchstabe a^{bis} (aus Art. 20 Abs. 2 MIG inhaltlich unverändert übernommener Katalog der bearbeiteten Personendaten);
- Artikel 16 Absatz 1 Einleitungssatz und Buchstabe b^{bis} (wie heute in Art. 22 Abs. 1 MIG für das ITR geregelt, sollen auch künftig die mit der Rekrutierung beauftragten Ärztinnen und Ärzte durch Abrufverfahren Zugang zu den für die

Aufgabenerfüllung benötigten Daten des PISA, insb. denjenigen nach Art. 14 Abs. 1 Bst. a^{bis}, haben);

- Artikel 17 Absatz 4ter (wie bisher im ITR [vgl. Art. 23 MIG] sind die an der Rekrutierung erhobenen sanitätsdienstlichen Daten [vgl. zum Begriff Art. 26 Abs. 2 MIG] in das MEDISA zu überführen und innert Wochenfrist nach der Datenerhebung im PISA wieder zu löschen);
- Die übrigen ITR-Bestimmungen sind in den PISA-Bestimmungen inhaltlich bereits abgedeckt.

Für die Integration der FallDok PPD sind Änderungen in den folgenden PISA-Bestimmungen erforderlich:

- Artikel 13 Buchstabe o (Zweck der Datenbearbeitung; entspricht Art. 37 Bst. a MIG);
- Artikel 14 Absatz 4 (bearbeitete Personendaten; entspricht Art. 38 MIG);
- Artikel 15 Absatz 4 (Datenbeschaffung; entspricht Art. 39 MIG);
- Artikel 16 Absatz 1ter (Datenbekanntgabe; entspricht Art. 40 Abs. 1 MIG – die gemäss dem heutigen Art. 40 Abs. 2 MIG bekanntzugebenden Daten werden von Art. 14 Abs. 1 MIG erfasst und können daher gemäss Art. 15 Abs. 1 Bst. d MIG beim Psychologisch-pädagogischen Dienst der Armee [PPD] beschafft und gestützt auf Art. 16 Abs. 1 Bst. a und b MIG den Militärbehörden und militärischen Kommandos bekanntgegeben werden);
- Artikel 17 Absatz 4^{quater} (Datenaufbewahrung; entspricht Art. 41 MIG, wobei mit dem neu hinzukommenden Wort «längstens» klargestellt werden soll, dass die Daten schon vor Ablauf von fünf Jahren gelöscht werden können und nicht zwingend fünf Jahre aufbewahrt werden müssen).

Weiter soll mit der vorgesehenen Ergänzung am Ende des Einleitungssatzes von Artikel 16 Absatz 1 dem Verhältnismässigkeitsgrundsatz bei der Datenbearbeitung (vgl. Art. 4 Abs. 2 aDSG bzw. künftig Art. 6 Abs. 2 nDSG) Rechnung getragen werden: Nicht zuletzt auch angesichts der erfolgenden Integration des ITR und der FallDok PPD sowie der damit unter anderem ins PISA fliessenden sanitätsdienstlichen Daten, ist die Bekanntgabe der PISA-Daten durch Abrufverfahren derart einzuschränken, dass sie 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 Art. 14 Abs. 1 Bst. a^{bis}), sondern nur die von ihnen tatsächlich benötigten sehen können.

Mit den Anpassungen in Artikel 13 Buchstabe f und Artikel 16 Absatz 1 Buchstabe h soll erreicht werden, dass die PISA-Daten nicht nur zur Verhinderung von Missbräuchen der Erwerbsersatzordnung, sondern generell zur Durchführung der Erwerbsersatzordnung bearbeitet und der Zentralen Ausgleichsstelle im vorgesehenen Umfang zugänglich gemacht werden dürfen. Denn die heute noch in Papierform einzureichenden Anmeldeformulare für Leistungen der Erwerbsersatzordnung sollen künftig im Rahmen der Digitalisierung der Erwerbsersatzordnung durch eine digitale Meldung,

etwa der geleisteten Diensttage, und eine informatikunterstützte Datenbearbeitung abgelöst werden. Dadurch können Prozesse automatisiert, die Auszahlung von Leistungen der Erwerbsersatzordnung beschleunigt und der Bearbeitungsaufwand reduziert werden. Eine solche digitale Durchführung der Erwerbsersatzordnung ist nur möglich, wenn die notwendigen PISA-Daten zu diesem Zweck bereitgestellt werden 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 von Anfragen zu Zahlen betreffend das VBS beigezogen werden dürfen. Überdies sollen auch Daten über absolvierte Ausbildungen und erlangte Berechtigungen von militärischen Systemen im PISA erfasst werden (vgl. Art. 14 Abs. 1 Bst. 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 erfassten PISA-Daten auch schon vor Ablauf von fünf Jahren (z. B. jahrgangsweise Löschung) möglich ist und eine fünfjährige Aufbewahrungsdauer nicht zwingend erforderlich ist.

Die Änderung in Artikel 14 Absatz 2 ist rein gesetzesredaktioneller Natur. Wie in den Absätzen 3 und (neu) 4 schliesst das Pronomen «Es» an «Das PISA» in Absatz 1 an.

Eine weitere Änderung betrifft den Wortlaut des Einleitungssatzes von Artikel 15 Absatz 1 im deutschen Text, der geschlechtergerecht formuliert werden soll. In Artikel 15 Absatz 2 Buchstabe a und Artikel 17 Absatz 1 Buchstabe e wird jeweils auf das am 1. Januar 2021 in Kraft getretene BZG verwiesen. Zudem ist in Artikel 16 Absatz 1 Buchstabe i die Abkürzung des NDG einzuführen, die später wiederverwendet wird (siehe Art. 147 Abs. 2 Bst. c und Art. 167*k* Abs. 2 Bst. g).

Art. 18–23 (Informationssystem ITR)

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

Art. 24; Art. 27 Einleitungssatz; Art. 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 1998[22] [RVOV]) erwähnt werden (in Art. 24 sowie in den Einleitungssätzen der Art. 27 sowie 28 Abs. 1 und 3). Die untergeordnete Verwaltungseinheit, die Inhaberin der Datensammlung und für den Datenschutz verantwortliches Bundesorgan ist, ist in den Ausführungsbestimmungen auf Verordnungsstufe zu definieren (vgl. Art. 2*a* und Anhang 1 MIV).

22 SR **172.010.1**

Die Änderung von Artikel 28 Absatz 1 Buchstabe c ist gesetzestechnisch bedingt (Verwendung der neu bereits in Art. 14 Abs. 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. Art. 2*a* 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. Art. 14 Abs. 4) können die bisherigen Bestimmungen zur FallDok PPD aufgehoben werden.

Art. 42; Art. 45 Einleitungssatz; Art. 46 Abs. 1 Einleitungssatz und Abs. 2; Art. 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. Art. 2*a* und Anhang 1 MIV).

Artikel 47 Absatz 1 ist aufzuheben, da gemäss Artikel 8 MIG und dem BGA das Bundesarchiv die nicht mehr ständig benötigten Unterlagen archiviert. 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. 48–50; Art. 51 Einleitungssatz, Art. 52 Abs. 1; Art. 53 Abs. 2 (Informationssystem Einsatzpersonal Kommando Spezialkräfte [ISEP KSK])

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 (Art. 49 Bst. a und b sowie 53 Abs. 2) sind daher derart auszugestalten, dass sämtliche vorgenannten Personen umfasst werden. Die Änderung in Artikel 49 Buchstabe c ist rein sprachlicher Natur und betrifft nur den französischen Text. Artikel 50 soll im deutschen Text sprachlich an den französischen und italienischen Text angepasst werden, indem sich «im Einsatz» neu nicht nur auf das Ausfallrisiko, sondern auch auf das Durchhaltevermögen bezieht.

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. Art. 2*a* 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 umfasst werden. Denn auch diese werden vom Sozialdienst der Armee gestützt auf die Verordnung vom 30. November 2018[23] 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-Nummer. 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.

Weiter sind in Artikel 58 Buchstabe b die beim Fachstab des Sozialdienstes der Armee eingeteilten Armeeangehörigen, die 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 Armeeangehörigen sind nicht Mitarbeitende (im Sinne von Arbeitnehmerinnen

23 SR **611.021**

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 Armeeangehörige anbieten, durch Abrufverfahren Zugriff jeweils nur auf die ihre eigenen Klientinnen und Klienten betreffenden Daten des ISB erhalten.

Art. 63 Abs. 2; Art. 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 2017[24] über den Schutz von Personendaten des Bundespersonals (BPDV) geregelte Informationssystem für das Personaldatenmanagement (IPDM) abgelöst. Entsprechend ist in Artikel 63 Absatz 2 das IPDM anstelle des BV PLUS als Datenbezugsquelle zu nennen. In Artikel 65 Absatz 2 ist überdies entsprechend der in Artikel 8 neu verwendeten Begrifflichkeit (vgl. Erläuterungen zu Art. 8) das Wort «gelöscht» durch «vernichtet» zu ersetzen; zudem wird mit Bezug auf die Kandidatinnen und Kandidaten die weibliche Form wie in anderen Bestimmungen des MIG vor der männlichen Form verwendet.

Art. 72; Art. 73 Einleitungssatz; Art. 75 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. Art. 2*a* und Anhang 1 MIV). Ferner ist die durch die Anpassung in Artikel 72 wegfallende Abkürzung «KSD» neu im Einleitungssatz von Artikel 73 einzuführen. In den Einleitungssätzen der Artikel 73 und 75 wird mit Bezug auf die Beauftragte oder den Beauftragten die weibliche Form wie in anderen Bestimmungen des MIG jeweils vor der männlichen Form verwendet.

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

Zur Durchführung der Erwerbsersatzordnung soll mit den zu ändernden Artikeln 85 Absatz 2 und 88 (neuer Bst. 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 bekanntgegeben 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

24 SR **172.220.111.4**

Kommando übermittelt werden können. Durch diese Möglichkeit werden die Abläufe im Zusammenhang mit der Verwaltung und dem Betrieb in Schulen und Kursen (so der in Art. 85 MIG genannte Zweck des MIL Office) für alle Beteiligten verkürzt und vereinfacht.

Mit den Anpassungen in Artikel 86 (Neuaufnahme der Bst. a und h; bisheriger Bst. a wird zu Bst. a^{bis}) werden die in den Ausführungsbestimmungen (vgl. Anhang 16 Ziff. 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.

Die Änderung in Artikel 88 Buchstaben a–c ist sprachlicher sowie gesetzesredaktioneller Natur und betrifft nur den französischen Text.

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. Zwecks sprachlicher Vereinheitlichung mit Blick auf die Artikel 93 und 95 sollen zudem die «betreffende Person» (anstatt die «betroffenen Mitarbeiterinnen und Mitarbeiter») und «ihre Vorgesetzten» (anstatt die «betroffenen Linienvorgesetzten») genannt werden.

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

Das FIS HE soll nicht mehr zur Aktionsführung, dafür aber zur Lageverfolgung eingesetzt werden können. Zudem soll es dem 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; Art. 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 Art. 8) das Wort «gelöscht» durch «vernichtet» zu ersetzen.

Art. 121; Art. 123 Einleitungssatz und Bst. c; Art. 124 Abs. 2 Bst. c; Art. 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. Dadurch lassen sich Ausbildungsresultate und erworbene Kompetenzen besser nachvollziehen, was zu einer besseren Aufgabenerfüllung beiträgt. Entsprechend ist in Artikel 125 Absatz 2 die bisherige fünfjährige Aufbewahrungsdauer auf zehn Jahre zu verlängern. Weiter ist in den einzelnen Bestimmungen (Art. 121, 123 Bst. c, 124 Abs. 2 und 125 Abs. 2) vorzusehen, dass die Daten aller Zivilpersonen und Dritten (etwa von Blaulichtorganisationen), die an den Simulatoren trainieren, bearbeitet und bei deren zivilen Vorgesetzten beschaffen bzw. diesen bekanntgegeben werden dürfen.

Art. 131 (Informationssystem LMS VBS)

Angehörige der Armee und Angestellte des VBS nehmen erfahrungsgemäss während etwa 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 Armeeangehörigen 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 Gefahrenguttransport oder Ladesicherung oder von eidgenössischen Schiessoffizierinnen und -offizieren im Bereich allgemeiner Sicherheitsvorschriften) zu verfügen und so eine Ausbildungskontrolle (vgl. Art. 127 Bst. d MIG) und das Kompetenzmanagement (vgl. Art. 127 Bst. 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; Art. 139 Einleitungssatz sowie Bst. a, c, e und f; Art. 140 Einleitungssatz und Bst. b–d; Art. 141 Einleitungssatz und Bst. b–e; Art. 142 Abs. 1; Art. 143 (Informationssystem FA-SVSAA)

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. Art. 32 und 38 der Verordnung vom 11. Februar 2004[25] über den militärischen Strassenverkehr [VMSV]) und Schiffsführerinnen und -führer (vgl. Art. 4 und 14 der Verordnung vom 1. März 2006[26] über die militärische Schifffahrt [VMSch]),

25 SR **510.710**
26 SR **510.755**

- der Ausweise der militärischen Verkehrsexpertinnen und -experten (bzw. Prüfungsexpertinnen und -experten), welche Prüfungen für Fahrzeug- (vgl. Art. 29 VMSV) und Schiffsführerinnen und -führer (vgl. Art. 4 VMSch) abnehmen,
- der eidgenössischen Schiffsführerinnen- und Schiffsführerausweise (vgl. Art. 3 und 11 der Verordnung vom 1. März 2006[27] 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»]) zu ändern. Zu ergänzen sind die vorgenannten Personengruppen bzw. Fahrberechtigungen und Ausweise – soweit noch nicht aufgeführt – in der Zweckbestimmung (Art. 139 Bst. a und c) und in der Bestimmung mit den zu bearbeitenden Personendaten (Art. 140 Bst. b). Ferner ist zudem als neue Datenbeschaffungsquelle insbesondere für Daten betreffend Eidgenössische Schiffsführerausweise das IPDM (vgl. Art. 30–38 BPDV) in Artikel 141 Buchstabe d zu nennen.

In Artikel 139 ist Buchstabe f aufzuheben, da heute keine Daten mehr zum dort genannten Zweck (Bewirtschaftung der Bescheinigungen nach dem Europäischen Übereinkommen vom 30. September 1957[28] über die internationale Beförderung gefährlicher Güter auf der Strasse) 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 2018[29] über das Informationssystem Verkehrszulassung) abgelöst und sind entsprechend zu ersetzen.

In Artikel 143 Absatz 1 soll die Aufbewahrung der Daten des FA-SVSAA, einschliesslich der Daten über militärische Administrativmassnahmen (Art der Administrativmassnahme, ihr Grund, ihre Dauer sowie die Stelle, welche die Administrativmassnahme verfügt und/oder erfasst hat), 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

27 SR **747.201.2**
28 SR **0.741.621**
29 SR **741.58**

Datenbeschaffungsquelle das IPV anzuführen ist: Anders als aus dem PISA können aus dem IPV insbesondere aktuelle Daten zu den Ausweisen von militärischen Verkehrsexpertinnen und -experten, die nicht mehr militärdienstpflichtig sind, bezogen werden. 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 so lange 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. Dies wird auch mit der Änderung in Artikel 140 Buchstaben c und d verdeutlicht.

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. 143c Bst. l (Informationssystem SPHAIR-Expert)

Für die Durchführung des in Artikel 2*b* Buchstabe g vorgesehenen Profilings sollen im SPHAIR-Expert mit dem in Artikel 143*c* neu einzufügenden Buchstaben l auch persönliche Interessen hinsichtlich der Anstellung, Ausbildung, Weiterentwicklung sowie Berufs- und Funktionswahl bearbeitet werden dürfen.

Art. 143g–143l (Informationssystem ISFA)

Um die künftig nach Artikel 34 Absatz 2 Buchstabe b nDSG für eine Datenbearbeitung durch «Profiling» und «Profiling mit hohem Risiko» erforderliche Grundlage in einem Gesetz im formellen Sinn zu schaffen, ist zusätzlich zur neuen Regelung in Artikel 2*b* das derzeit nur auf Verordnungsstufe geregelte Informationssystem Führungsausbildung (ISFA) neu im MIG zu regeln. Gestützt auf die neu einzuführenden Artikel 143*g*-143*l* MIG wird die Datenbearbeitung im ISFA im gleichen Umfang wie bisher gestützt auf die entsprechenden Bestimmungen in der MIV (Art. 62 ff. und Anhang 29 MIV) möglich sein.

Art. 145; Art. 147 Abs. 2 Einleitungssatz sowie Bst. c und d; Art. 148 Abs. 1 Einleitungssatz sowie Bst. c Ziff. 2bis und Bst. d (Informationssystem SIBAD)

Die Anpassung von Artikel 145 soll den unterschiedlichen Benennungen und auch Zwecken der Prüfungen, Beurteilungen und Kontrollen, wie sie auf Gesetzesstufe erwähnt sind, Rechnung tragen. Zu diesen gehören beispielsweise Personensicherheitsprüfungen nach den Artikeln 19–21 des Bundesgesetzes vom 21. März 1997[30] über

[30] SR **120**

Massnahmen zur Wahrung der inneren Sicherheit, nach den Artikeln 23 und 103 MG und nach Artikel 20*a* des Stromversorgungsgesetzes vom 23. März 2007[31] (StromVG), Beurteilungen des Gefährdungs- oder Missbrauchspotenzials bezüglich der persönlichen Waffe nach Artikel 113 MG und Zuverlässigkeitskontrollen nach Artikel 24 des Kernenergiegesetzes vom 21. März 2003[32].

Zwecks begrifflicher Vereinheitlichung innerhalb des MIG ist im Einleitungssatz von Artikel 147 Absatz 2 «im Umfang (der entsprechenden Rechtsgrundlagen)» durch «im Rahmen (der entsprechenden Rechtsgrundlagen)» zu ersetzen (vgl. so auch Art. 183 Abs. 2 MIG).

In Artikel 147 Absatz 2 Buchstabe c ist als Datenbeschaffungsquelle das Informationssystem INDEX NDB anstelle des nicht mehr existierenden Staatsschutz-Informations-Systems zu nennen.

Die Rechtsgrundlagen für einen Zugriff durch Abrufverfahren auf Daten aus diversen Datenbanken der Zentralstelle Waffen nach Artikel 32*a* Absatz 1 des Waffengesetzes vom 20. Juni 1997[33] (WG) (Waffeninformationsplattform ARMADA) existieren bereits. Sie befinden sich in Artikel 32*c* Absatz 8 WG i.V.m. Artikel 61 Absatz 2 Buchstabe e und Artikel 61 Absatz 6 i.V.m. Anhang 3 der Waffenverordnung vom 2. Juli 2008[34] (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 von Artikel 147 Absatz 2 den Zugang 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 2bis die nationale Netzgesellschaft aufzuführen, da gemäss dem am 1. Januar 2018 in Kraft getretenen Artikel 20*a* 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 20*a* Absatz 3 StromVG vorgesehene Mitteilung der Ergebnisse der Personensicherheitsprüfungen erleichtert. Die nationale Netzgesellschaft könnte selber die Daten aus dem SIBAD abrufen, wobei im Sinne des gemäss Artikel 1 Absatz 3 MIG i.V.m. Artikel 4 Absatz 2 aDSG (bzw. künftig Art. 6 Abs. 2 nDSG) 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

31 SR **734.7**
32 SR **732.1**
33 SR **514.54**
34 SR **514.541**

mit Sicherheitsaufgaben beauftragten Stellen des Bundes durch Abrufverfahren zugänglich sind, die sich bei ihrer Tätigkeit auf diese Daten stützen müssen. Zudem soll auch nur der Zugang auf die für die betreffende Person nicht nachteiligen Daten möglich sein.

Die vorgesehenen Änderungen der Bestimmungen zum SIBAD sollen nur erfolgen, sofern und solange das Informationssicherheitsgesetz vom 18. Dezember 2020[35] (ISG) noch nicht in Kraft getreten ist. Denn das ISG wird nebst den Bestimmungen des MIG zum Informationssystem Industriesicherheitskontrolle (ISKO, Art. 150–155) unter anderem auch diejenigen zum SIBAD (Art. 144–149) aufheben und neu die informationssystem- und datenschutzrelevanten Regelungen enthalten. Die nötige Koordinationsbestimmung ist in die vorliegende Änderung des MIG aufzunehmen (siehe Ziff. 5.2); sie hat klarheitshalber die im ISG unter ein und derselben Anweisung enthaltene Regelung zu wiederholen, wonach die Artikel 144–155 MIG zu den Informationssystemen ISKO und SIBAD aufgehoben werden.

Gliederungstitel vor Art. 167a; Art. 167a; Art. 167b Bst. a und b; Art. 167d; Art. 167e Abs. 1 und 2 Bst. b und c; Art. 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 167*d* Buchstabe e ist einerseits die Regelung des bisherigen Artikels 167*d* Absatz 2 MIG integriert, wobei für das MIFA die neu einzuführende Abkürzung FASVSAA (vgl. Erläuterungen zu Art. 138 ff.) zu verwenden ist. Weiter soll im Einleitungssatz des Artikels 167*d* Buchstabe e explizit geregelt werden, dass die Datenbeschaffung aus allen in Artikel 167*d* Buchstabe e genannten Informationssystemen (insb. auch den unter den Ziff. 2–7 und 9 neu aufgenommenen) möglich ist, sei es manuell durch Abrufverfahren (in der Regel über eine von den Betreibern des jeweiligen Informationssystems bereitgestellte Web-Schnittstelle oder über eine spezifische Software) oder automatisiert über eine (geplante) Schnittstelle, über welche die Daten automatisch übernommen werden können. Dadurch kann die Beschaffung der Personendaten beschleunigt und vereinfacht werden, die für die tägliche Aufgabenerfüllung (z. B. 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. Im Einzelnen gewähren die neu in Artikel 167*d* Buchstabe e aufgenommenen Informationssysteme Zugang zu den folgenden Daten:

35 BBl **2020** 9975

(Neu aufgenommenes) **Informationssystem**	**Gewährt Zugang zu folgenden Daten:**
RIPOL (Art. 167*d* Bst. e Ziff. 2)	Daten zu ungeklärten Straftaten (z. B. als gestohlen gemeldete Gegenstände) (vgl. Art. 3 Bst. h, 6 Abs. 1 Bst. o, 7 Abs. 1 sowie Anhang 1 Ziff. 2 der Verordnung vom 26. Oktober 2016[36] über das automatisierte Polizeifahndungssystem [RIPOL-Verordnung])
IVZ (Art. 167*d* Bst. e Ziff. 3)	Daten zu Fahrzeugen und deren Verkehrszulassung, zu Fahrzeugführerinnen und -führern sowie deren Fahrberechtigung, zu Fahrzeughalterinnen und -haltern sowie zu Motorfahrzeugversicherungen (vgl. Art. 89*e* Bst. a des Strassenverkehrsgesetzes vom 19. Dezember 1958[37] [SVG])
Datenbanken der Zentralstelle Waffen nach Artikel 32*a* WG (Art. 167*d* Bst. e Ziff. 4)	Online-Zugang zu den Daten der Datenbanken der Zentralstelle Waffen nach Artikel 32*a* WG, um zu überprüfen, ob einer Person der Erwerb von Waffen untersagt oder ihr die Waffe abgenommen wurde (vgl. Art. 32*a*–32*c* WG)
Online-Abfrage Waffenregister der Kantone (Art. 167*d* Bst. e Ziff. 5)	Online-Abfrage in den kantonalen Registern der Feuerwaffenbesitzerinnen und -besitzer (Daten über den Erwerb und Besitz von Feuerwaffen) (vgl. Art. 32*a* Abs. 2 und 3 sowie 32*b* Abs. 6 WG)
PISA (Art. 167*d* Bst. e Ziff. 6)	Militärische Daten wie Einteilung, Grad, Funktion und Dienstleistungen in der Armee (vgl. Art. 167*c* Abs. 1 Bst. d)
IPV (Art. 167*d* Bst. e Ziff. 7)	Daten wie Funktion, Ausbildung, Einsatz in der Armee, militärischer Status, berufliche Laufbahn, Sprachkenntnisse (vgl. Art. 62 Bst. b–e und g MIG)
DDSV (Art. 167*d* Bst. e Ziff. 9)	Daten wie Einteilung, Grad, Funktion, Ausbildung, Qualifikation und Ausrüstung in der Armee und im Zivilschutz (vgl. Art. 176 Bst. a MIG)

Da Artikel 100 MG mehrere Aufgaben nennt, die von den Mitarbeiterinnen und Mitarbeitern des Kommandos Militärpolizei zu erfüllen sind, ist in Artikel 167*e* Absatz 1 Buchstabe b eine entsprechende Änderung von der Einzahl «Aufgabe» zur Mehrzahl «Aufgaben» vorzunehmen. Weiter sind in Artikel 167*e* Absatz 1 Buchstabe c der Einfachheit und Klarheit halber die Mitarbeiterinnen und Mitarbeiter des DPSA 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. Art. 100 Abs. 1 Bst. a und e MG sowie Art. 11 VMS).

36 SR **361.0**
37 SR **741.01**

Der Artikel 167*e* Absatz 2 Buchstabe b ist geschlechtergerecht zu formulieren. In Artikel 167*e* Absatz 2 Buchstabe c ist nicht eine bestimmte, für die Informations- und Objektsicherheit zuständige Stelle (wie etwa die organisatorisch dem Generalsekretariat des VBS zugehörige Informations- und Objektsicherheit) zu nennen, sondern es sollen sämtliche für die Informations- und Objektsicherheit zuständigen Stellen (insb. 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 Text.

Art. 167g–167l (Informationssystem IPSA)

Mit den neu einzuführenden Artikeln 167*g*–167*l* soll eine Rechtsgrundlage für das Informationssystem IPSA geschaffen werden. Dieses soll dem DPSA zur Erfüllung seiner Aufgaben dienen, insbesondere zur Beurteilung der militärischen Sicherheitslage und zum vorsorglichen Schutz der Armee vor Spionage, Sabotage und weiteren rechtswidrigen Handlungen (vgl. Art. 100 Abs. 1 Bst. a und e MG sowie Art. 11 VMS) sowie zur Journal- und Einsatzführung. Damit sich die vorgenannten Aufgaben optimal erfüllen lassen, ist es notwendig, die Personen, von denen eine mögliche Bedrohung der Armee ausgeht (Art. 167*i* Einleitungssatz), samt Detailangaben zu dieser Bedrohung (Art. 167*i* Bst. m) im IPSA erfassen zu können.

Im IPSA müssen für die Aufgabenerfüllung auch besonders schützenswerte Personendaten bearbeitet werden. Zu diesen gehören etwa:

- die ethnische und religiöse Zugehörigkeit (vgl. Art. 167*i* Bst. c; benötigt für die Einschätzung möglicher Motive in den Bereichen Gewaltextremismus, Terrorismus und Spionage gegen die Armee);
- die politische und ideologische Ausrichtung (vgl. Art. 167*i* Bst. e; benötigt für die Einschätzung möglicher Motive in den Bereichen Gewaltextremismus, Terrorismus und Spionage gegen die Armee);
- medizinische und biometrische Daten (vgl. Art. 167*i* Bst. h; benötigt etwa für die eindeutige Identifizierung von Personen oder für die Erfassung psychischer Erkrankungen, die einen Einfluss auf die Sicherheit der Armee haben könnten);
- weitere, auch besonders schützenswerte Personendaten (vgl. Art. 167*i* Bst. n, Art. 100 Abs. 3 Bst. a MG).

Damit diese besonders schützenswerten Personendaten im IPSA bearbeitet werden dürfen, bedarf es gemäss Artikel 17 Absatz 2 aDSG (bzw. Art. 34 Abs. 2 Bst. a nDSG) einer Rechtsgrundlage in einem formellen Gesetz.

Bei den Bezugspersonen, deren Daten und Identitäten im IPSA ebenfalls bearbeitet werden (Art. 167*i* Bst. j), handelt es sich um Personen, die zwar selbst keine Bedro-

hung für die Armee darstellen müssen, die jedoch einen Bezug zu einer Person aufweisen, von der eine mögliche Bedrohung der Armee ausgeht. 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 167*j* Buchstaben a–f genannten Quellen auch durch Abrufverfahren aus den unter Artikel 167*j* Buchstabe g genannten Informationssystemen permanent möglich sein, damit der DPSA die zur Aufgabenerfüllung erforderlichen Personendaten jederzeit schnell und einfach beschaffen kann. Angesichts der allgemein gehaltenen Formulierung fallen unter die gemäss Artikel 167*j* beschaffbaren Daten sämtliche, die im IPSA zu den Zwecken gemäss Artikel 167*h* bearbeitet werden dürfen, ungeachtet davon, wie sie von der bekanntgebenden Seite beschafft wurden. Irrelevant für die Beschaffbarkeit von Daten bei Nachrichtendiensten gestützt auf Artikel 167*j* Buchstabe c ist insbesondere, mit welchen Beschaffungsmassnahmen und -methoden der bekanntgebende Nachrichtendienst die bekanntzugebenden Daten erlangt hat und ob diese Massnahmen und Methoden genehmigungspflichtig waren oder nicht.

Gliederungstitel vor Art. 168; Art. 168; Art. 169 Einleitungssatz sowie Bst. d und e; Art. 170 Einleitungssatz sowie Bst. a und a^{bis}; Art. 171 Einleitungssatz und Bst. i; Art. 172; Art. 173 (Informationssystem Schadenzentrum [SCHAMIS])

Die Anpassung des Gliederungstitels vor Artikel 168 betrifft nur den französischen und den italienischen Text und ist rein sprachlicher Natur.

Das Generalsekretariat des VBS arbeitet mit der Nachfolgeanwendung des seit Ende 2003 betriebenen SCHAWE. 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 festzuhalten, denen das SCHAMIS dient:

- Zum einen erfolgt die Schadenregulierung bei Unfällen und Schadenfällen im Zusammenhang mit Bundesfahrzeugen nach Artikel 21 der Verordnung vom 23. Februar 2005[38] 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 1959[39] zuhanden der kantonalen Fahrzeugzulassungsstellen (Strassenverkehrsämter) aus. Neu kann dieser Arbeitsschritt über die Anwendung SCHAMIS verarbeitet und daher in die Zweckbestimmung des Gesetzes (Art. 169 Bst. d) aufgenommen werden.

38 SR **514.31**
39 SR **741.31**

- Zum anderen wird die Regulierung von Schadenfällen von Motorfahrzeugen von Ratsmitgliedern nach Artikel 4 Absatz 2 der Verordnung der Bundesversammlung vom 18. März 1988[40] zum Parlamentsressourcengesetz über die Anwendung SCHAMIS abgewickelt, was in der entsprechenden Zweckbestimmung des Gesetzes (Art. 169 Bst. 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. Art. 170 Bst. a^{bis}).

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 genannt werden.

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

Gliederungstitel vor Art. 174; Art. 174; Art. 175 Einleitungssatz; Art. 176 Einleitungssatz und Bst. c; Art. 177 Einleitungssatz; Art. 178; Art. 179 (Informationssystem Datendrehscheibe Verteidigung [DDSV])

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 auszutauschen sind, gehören auch besonders schützenswerte Personendaten (vgl. die Definition des Begriffs «Daten» in Art. 1 Abs. 1).

In Artikel 178 ist zu präzisieren, welche im DDSV bearbeiteten Personendaten welchen Stellen und Personen bekanntgegeben werden dürfen. So sollen die im DDSV

40 SR **171.211**

für den Datenaustausch zwischen den militärischen Informationssystemen bearbeiteten Personendaten nur denjenigen Stellen und Personen bekanntgegeben werden, die auch für die vom Datenaustausch jeweils betroffenen militärischen Informationssysteme zuständig sind. Einzig die Personendaten nach Artikel 176 Buchstaben a und b sind für die Bekanntgabe an militärische Kommandos sowie an zuständige Verwaltungseinheiten des Bundes und der Kantone gedacht.

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

In Artikel 179*c* Absatz 4 soll nicht mehr auf die beiden Artikel des Bundespersonalgesetzes vom 24. März 2000[41] (BPG) verwiesen werden, die am 1. Januar 2018 aufgehoben worden sind, sondern lediglich in unspezifischer Weise auf das BPG und dessen Ausführungsbestimmungen (vgl. Art. 8 ff. BPDV für das Bewerbungsdossier und Art. 19 ff. BPDV für das Personaldossier).

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 179*e* Absatz 2 Buchstabe e das IPDM anstelle des BV PLUS zu nennen.

Die Änderung von Artikel 179*b* Buchstabe d ist bloss formeller Art und gesetzestechnisch bedingt (Verwendung der bereits zuvor in Art. 16 Abs. 3bis eingeführten Abkürzung «WG»); sie betrifft nur den deutschen Text.

Gliederungstitel vor Art. 179g; Art. 179g; Art. 179h Einleitungssatz; Art. 179i Einleitungssatz; Art. 179j Einleitungssatz; Art. 179k Abs. 1 Einleitungssatz und Abs. 2; Art. 179l Abs. 1 (Informationssystem SaD)

Bezeichnung und Abkürzung des Informationssystems sind in Anpassung an die zukünftige Systemlösung von «Informationssystem Vereins- und Verbandsadministration (VVAdmin)» zu «Informationssystem Schiesswesen ausser Dienst (SaD)» zu ändern.

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 von künftig möglichen, etwa an einem Vertragsabschluss interessierten Geschäftspartnerinnen und Geschäftspartnern (vgl. Art. 179*o*) für die Geschäftsprozesse in den Bereichen Finanzen, Beschaffung, Logistik, Immobilien und Personal verwaltet und bereitgestellt werden (Art. 179*n*) – sogenannte «Stammdaten» (*«Master Data»*). Zu diesen Daten gehört auch die «Sozialversicherungsnummer» (Art. 179*o* Bst. k), worunter sowohl die AHV-Nummer als auch ausländische Sozialversicherungsnummern von Geschäftspartnerinnen und Geschäftspartnern aus dem Ausland fallen. Geschäftspartnerinnen und Geschäftspartner können sowohl Privatpersonen

41 SR **172.220.1**

als auch Unternehmen sein. Unter die «künftig möglichen» Geschäftspartnerinnen und Geschäftspartner fällt, wer etwa aufgrund einer Kontaktaufnahme oder Interessensbekundung mit einer gesteigerten Wahrscheinlichkeit künftig in einen Geschäftsprozess des VBS in den Bereichen Finanzen, Beschaffung, Logistik, Immobilien oder Personal involviert sein wird. Alle anderen, bei denen sich eine solche gesteigerte Wahrscheinlichkeit nicht begründen lässt, werden nicht als «künftig mögliche» Geschäftspartnerinnen und Geschäftspartner ins MDM aufgenommen. 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 Informationsschutzbedürfnisse 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 (sog. «Once-only-Prinzip»), nicht verwaltungsspezifisch angereicherten Daten für das MDM zu beschaffen (vgl. Art. 179*p* Bst. 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 Finanzhaushaltgesetzes vom 7. Oktober 2005[42] und dessen Ausführungsbestimmungen) vorzusehen (Art. 179*r* Abs. 1 Bst. b). Steht fest, dass eine Person, die zunächst als künftig mögliche Geschäftspartnerin bzw. künftig möglicher Geschäftspartner im MDM erfasst wurde, nun doch nicht Geschäftspartnerin oder Geschäftspartner wird, sind deren Daten ab diesem Zeitpunkt zwecks Nachvollziehbarkeit des Verwaltungshandelns und der getroffenen Entscheide nur während zwei Jahren aufzubewahren (Art. 179*r* Abs. 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 berichtigend 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 zugunsten der zivilen Behörden erbringen kann.

42 SR **611.0**

Art. 186 Abs. 3

Um internationale Abkommen abschliessen zu dürfen, die als Rechtsgrundlage für eine grenzüberschreitende Bearbeitung von solchen Personendaten dienen, deren Bearbeitung gemäss aDSG keine Grundlage in einem Gesetz im formellen Sinn erfordert, soll dem Bundesrat in Artikel 186 Absatz 3 die entsprechende Kompetenz eingeräumt werden. Diese Kompetenzeinräumung ermöglicht auch den Abschluss internationaler Abkommen durch den Bundesrat im Rahmen der im neuen Artikel 6 Buchstabe b genannten internationalen Zusammenarbeit (vgl. Erläuterungen zu Art. 6).

4.2 Militärgesetz (MG)

Art. 146 Militärische Informationssysteme

Der in Artikel 146 MG enthaltene Verweis auf das MIG ist aufgrund des geänderten Titels des MIG (vgl. die Erläuterungen zu dessen Erlasstitel) anzupassen.

Zudem soll sich dieser Verweis neu und allgemein auf die Bearbeitung aller, auch nichts besonders schützenswerter Personendaten beziehen (vgl. Erläuterungen zu Art. 1 Abs. 1 MIG). Denn das MIG enthält auch Bestimmungen über die Bearbeitung von Personendaten, die nicht besonders schützenswert sind. Damit diese nötige Anpassung mit dem künftigen Inkrafttreten des nDSG, das noch eine inhaltlich weniger allgemeine Formulierung von Artikel 146 MG vorsah, nicht wieder rückgängig gemacht wird, ist in der vorliegenden Änderung des MIG die erforderliche Koordinationsbestimmung vorzusehen (siehe Ziff. 5.1).

4.3 Informationssicherheitsgesetz (ISG)

Art. 45 Abs. 3bis und 6 Bst. d

Mit dem Inkrafttreten des ISG werden die Bestimmungen des MIG zum Informationssystem SIBAD (Art. 144–149) aufgehoben und die notwendigen informationssystem- und datenschutzrelevanten Bestimmungen im ISG selbst geregelt.

Die in dem neuen Artikel 2*b* Buchstabe h MIG und dem neuen Artikel 147 Absatz 2 Buchstabe d MIG vorgesehenen Regelungen (siehe die Erläuterungen hierzu) sind im ISG noch nicht enthalten. Das ISG ist daher gleichermassen um einen Artikel 45 Absatz 3bis (entspricht der Regelung in Art. 2*b* Bst. h MIG) und um einen Artikel 45 Absatz 6 Buchstabe d (entspricht der Regelung in Art. 147 Abs. 2 Bst. d MIG) zu ergänzen.

Ferner ist die Präzisierung des Datenbearbeitungszwecks im neuen Artikel 145 MIG, die im ISG ebenfalls noch nicht enthalten ist, auch in Artikel 45 Absatz 1 ISG vorzusehen. Zusätzlich zu den im neuen Artikel 145 MIG bereits genannten Zwecken sind in Artikel 45 Absatz 1 ISG zudem die Prüfungen der Vertrauenswürdigkeit zu nennen,

die in den mit dem ISG ebenfalls einzufügenden oder ändernden Artikel 29*a* des Asylgesetzes vom 26. Juni 1998[43], Artikel 20*b* BPG, Artikel 14 MG und Artikel 20*a* StromVG neu vorgesehen sein werden.

5 Koordination mit anderen Erlassen

Zwecks Koordination mit dem nDSG und dem ISG sind die erforderlichen Koordinationsbestimmungen wie folgt vorzusehen:

5.1 Koordination mit dem nDSG

Koordination mit dem Datenschutzgesetz vom 25. September 2020[44]

1. Unabhängig davon, ob zuerst das Datenschutzgesetz vom 25. September 2020[45] oder die vorliegende Gesetzesänderung in Kraft tritt, lauten mit Inkrafttreten des später in Kraft tretenden Gesetzes sowie bei gleichzeitigem Inkrafttreten die nachstehenden Bestimmungen des Bundesgesetzes vom 3. Oktober 2008[46] über die militärischen Informationssysteme wie folgt:

Art. 1 Abs. 1 Einleitungssatz und Abs. 3

1 Dieses Gesetz regelt die Bearbeitung von Personendaten natürlicher und juristischer Personen (Daten), einschliesslich besonders schützenswerter Personendaten, in Informationssystemen und beim Einsatz von Überwachungsmitteln der Armee und des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS) durch:

3 Soweit dieses Gesetz keine besonderen Bestimmungen enthält, ist das Datenschutzgesetz vom 25. September 2020[47] (DSG) anwendbar.

Art. 11

Aufgehoben

43 SR **142.31**
44 BBl **2020** 7639
45 BBl **2020** 7639
46 SR **510.91**
47 SR **235.1**

2. Unabhängig davon, ob zuerst das Datenschutzgesetz vom 25. September 2020[48] oder die vorliegende Gesetzesänderung in Kraft tritt, lautet mit Inkrafttreten des später in Kraft tretenden Gesetzes sowie bei gleichzeitigem Inkrafttreten die nachstehende Bestimmung des Militärgesetzes vom 3. Februar 1995[49] wie folgt:

Art. 146 Militärische Informationssysteme

Die Bearbeitung von Personendaten in Informationssystemen und beim Einsatz von Überwachungsmitteln der Armee und der Militärverwaltung wird im Bundesgesetz vom 3. Oktober 2008[50] über militärische und andere Informationssysteme im VBS geregelt.

5.2 Koordination mit dem ISG

Koordination mit dem Informationssicherheitsgesetz vom 18. Dezember 2020[51]

Unabhängig davon, ob zuerst das Informationssicherheitsgesetz vom 18. Dezember 2020[52] oder die vorliegende Gesetzesänderung in Kraft tritt, lauten mit Inkrafttreten des später in Kraft tretenden Gesetzes sowie bei gleichzeitigem Inkrafttreten die nachstehenden Bestimmungen des Bundesgesetzes vom 3. Oktober 2008[53] über die militärischen Informationssysteme wie folgt:

Art. 2b Bst. h

Die verantwortlichen Organe nach diesem Gesetz dürfen ein Profiling, einschliesslich eines Profilings mit hohem Risiko, durchführen, um die nachfolgenden persönlichen Aspekte einer natürlichen Person zu den nachstehenden Bearbeitungszwecken zu analysieren, zu bewerten, zu beurteilen oder vorherzusagen:

h. Sicherheitsrisiko sowie Gefährdungs- und Missbrauchspotenzial bezüglich der persönlichen Waffe: zum Bearbeitungszweck nach Artikel 13 Buchstabe l;

5. Kapitel 1. und 2. Abschnitt (Art. 144–155)

Aufgehoben

48 BBl **2020** 7639
49 SR **510.10**
50 SR **510.91**
51 BBl **2020** 9975
52 BBl **2020** 9975
53 SR **510.91**

6 Auswirkungen

6.1 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, damit Personendaten, die bearbeitet werden müssen, um öffentliche Aufgaben zu erfüllen, auch bearbeitet werden dürfen. Allfällige nötige, insbesondere (informatik-)technische Arbeiten erfolgen im Rahmen der laufenden Anpassungen und (Weiter-)Entwicklungen der Systeme.

6.2 Andere Auswirkungen

Die Massnahmen und Anpassungen der vorliegenden Botschaft 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.

7 Rechtliche Aspekte

7.1 Verfassungsmässigkeit

Mit Bezug auf die im MIG bereits geregelten militärischen Informationssysteme stützt sich die Regelungskompetenz des Bundes insbesondere auf Artikel 60 Absatz 1 BV, der die Militärgesetzgebung sowie Organisation, Ausbildung und Ausrüstung der Armee als Sache des Bundes bezeichnet. Zudem ergibt sie sich mit Bezug auf die Bearbeitung von Personendaten von Auslandschweizerinnen und Auslandschweizern auch aus 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 (und die in ihnen bearbeiteten Personendaten) dienen der Wahrnehmung von anderweitig verankerten Bundesaufgaben, die das VBS erfüllen muss. Ihre Regelung ist daher letztlich eine Frage der Organisation der Verwaltungseinheiten des VBS, wofür diese bzw. der Bund zuständig sind.

7.2 Vereinbarkeit mit internationalen Verpflichtungen der Schweiz

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

7.3 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 aDSG (bzw. Art. 34 Abs. 2 Bst. a nDSG) eine Grundlage in einem formellen Gesetz.

7.4 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.

7.5 Einhaltung des Subsidiaritätsprinzips und des Prinzips der fiskalischen Äquivalenz

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

7.6 Einhaltung der Grundsätze der Subventionsgesetzgebung

Die beantragten Gesetzesänderungen sehen keine Finanzhilfen oder Abgeltungen im Sinne des Subventionsgesetzes vom 5. Oktober 1990[54] vor.

7.7 Delegation von Rechtsetzungsbefugnissen

Rechtsetzungsbefugnisse können durch Bundesgesetz übertragen werden, soweit dies nicht durch die Bundesverfassung ausgeschlossen wird (Art. 164 Abs. 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.

7.8 Datenschutz

Die vorgesehenen Änderungen betreffen auch die Bearbeitung besonders schützenswerter Personendaten. Nach Artikel 17 Absatz 2 aDSG (bzw. Art. 34 Abs. 2 Bst. a nDSG) dürfen Bundesorgane besonders schützenswerte Personendaten grundsätzlich nur dann bearbeiten, wenn ein Gesetz im formellen Sinn dies vorsieht. Um die für die Aufgabenerfüllung notwendige Bearbeitung und den Austausch von Personendaten sicherzustellen, bedarf es aus datenschutzrechtlicher Sicht der in dieser Botschaft vorgesehenen Anpassungen bestehender Rechtsgrundlagen.

54 SR **616.1**

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesgesetz über die militärischen Informationssysteme (MIG)

Entwurf

Änderung vom …

Die Bundesversammlung der Schweizerischen Eidgenossenschaft,
nach Einsicht in die Botschaft des Bundesrates vom …[1],
beschliesst:

I

Das Bundesgesetz vom 3. Oktober 2008[2] über die militärischen Informationssysteme wird wie folgt geändert:

Titel

Bundesgesetz über militärische und andere Informationssysteme im VBS (MIG)

Ingress

gestützt auf die Artikel 40 Absatz 2, 60 Absatz 1 und 173 Absatz 2 der Bundesverfassung[3],

Ersatz eines Ausdrucks

Im ganzen Erlass wird «AHV-Versichertennummer» *durch* «AHV-Nummer» *ersetzt.*

Art. 1 Abs. 1 Einleitungssatz und Bst. b–d sowie Abs. 2 und 3

[1] Dieses Gesetz regelt die Bearbeitung von Personendaten natürlicher und juristischer Personen (Daten), einschliesslich besonders schützenswerter Personendaten, in Informationssystemen und beim Einsatz von Überwachungsmitteln der Armee und des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS) durch:

1 BBl **…** …
2 SR **510.91**
3 SR **101**

b. Kommandantinnen, Kommandanten und Kommandostellen der Armee (militärische Kommandos) sowie Kommandantinnen und Kommandanten des Zivilschutzes;

c. weitere Angehörige der Armee und des Zivilschutzes;

d. Dritte, die Aufgaben im Zusammenhang mit dem Militär- und Zivilschutzwesen oder für das VBS erfüllen.

2 Es gilt nicht für die Datenbearbeitung durch die Nachrichtendienste.

3 Soweit dieses Gesetz keine besonderen Bestimmungen enthält, ist das Bundesgesetz vom 19. Juni 1992[4] über den Datenschutz (DSG) anwendbar.

Art. 2 Abs. 1 Einleitungssatz und Bst. a

1 Soweit es zur Erfüllung ihrer gesetzlichen oder vertraglichen Aufgaben notwendig ist, dürfen die Stellen und Personen nach Artikel 1 Absatz 1 beim Betrieb von Informationssystemen oder beim Einsatz von Überwachungsmitteln der Armee und des VBS:

a. *Aufgehoben*

Art. 2b Profiling

Die verantwortlichen Organe nach diesem Gesetz dürfen ein Profiling, einschliesslich eines Profilings mit hohem Risiko, durchführen, um die nachfolgenden persönlichen Aspekte einer natürlichen Person zu den nachstehenden Bearbeitungszwecken zu analysieren, zu bewerten, zu beurteilen oder vorherzusagen:

a. Tauglichkeit und Fähigkeit für die Leistung von Militär- und Schutzdienst, einschliesslich tauglichkeits- und fähigkeitsrelevanter Voraussetzungen: zu den Bearbeitungszwecken nach Artikel 13 Buchstaben b–d;

b. Eignung zur Ausübung bestimmter Funktionen, Tätigkeiten und Arbeiten, einschliesslich eignungsrelevanter Voraussetzungen: zu den Bearbeitungszwecken nach den Artikeln 13 Buchstaben b–d und 143*b* Buchstaben d und e;

c. Leistungsprofil und Leistungsfähigkeit, insbesondere in den Bereichen Gesundheit, Körper, Intelligenz, Persönlichkeit, Psyche, Sozialverhalten und Verkehrsverhalten: zu den Bearbeitungszwecken nach den Artikeln 13 Buchstaben b–d und 143*b* Buchstaben d und e;

d. Kenntnisse, Kompetenzen, Fähigkeiten und erbrachte Leistungen: zu den Bearbeitungszwecken nach den Artikeln 13 Buchstaben b–d, 127 Buchstaben d und e, 143*b* Buchstaben d und e und 143*h*;

e. Lernverhalten und -fortschritt: zu den Bearbeitungszwecken nach Artikel 127 Buchstaben a–c;

f. Kaderpotenzial und Entwicklungsmöglichkeiten: zu den Bearbeitungszwecken nach Artikel 13 Buchstaben b–d und m;

4 SR **235.1**

g. persönliche Interessen hinsichtlich des Militär- und Schutzdienstes, der Anstellung, der Ausbildung sowie der Weiterentwicklung: zu den Bearbeitungszwecken nach den Artikeln 13 Buchstaben b–d und m, 127 Buchstabe b und 143*b* Buchstaben a, d und e;

h. Sicherheitsrisiko sowie Gefährdungs- und Missbrauchspotenzial bezüglich der persönlichen Waffe: zu den Bearbeitungszwecken nach den Artikeln 13 Buchstabe l und 145;

i. weitere persönliche Aspekte zu weiteren Bearbeitungszwecken, sofern die betreffende Person dazu einwilligt.

Art. 3

Aufgehoben

Art. 4 Abs. 1

1 Das VBS und seine Verwaltungseinheiten betreiben gemeinsam einen Verbund der in diesem Gesetz und dessen Ausführungsbestimmungen geregelten Informationssysteme.

Art. 6 Datenbearbeitung im Rahmen der internationalen Zusammenarbeit

Die zuständigen Behörden und militärischen Kommandos dürfen im Rahmen der Zusammenarbeit mit Behörden und militärischen Kommandos anderer Länder sowie internationalen Organisationen Daten bearbeiten und insbesondere durch Abrufverfahren bekannt geben, wenn dies:

a. in einem Gesetz im formellen Sinn oder einem Staatsvertrag, der dem fakultativen Referendum unterstand, vorgesehen ist;

b. in den vom Bundesrat erlassenen Ausführungsbestimmungen zu diesem Gesetz oder in einem vom Bundesrat abgeschlossenen internationalen Abkommen vorgesehen ist und für die Bearbeitung dieser Daten gemäss DSG[5] keine Grundlage in einem Gesetz im formellen Sinn erforderlich ist.

Art. 7 Abs. 2 erster Satz

2 Die mit Wartungs-, Unterhalts- oder Programmieraufgaben betrauten Personen, einschliesslich beigezogener externer Leistungserbringerinnen und Leistungserbringer, dürfen Daten bearbeiten, soweit dies zur Erfüllung der Aufgaben erforderlich ist und die Datensicherheit gewährleistet ist. …

Art. 8 Aufbewahrung, Archivierung und Vernichtung der Daten

1 Die Daten werden nur so lange aufbewahrt, wie es der Bearbeitungszweck erfordert.

5 SR **235.1**

2 Nicht mehr benötigte Daten werden dem Bundesarchiv zur Archivierung angeboten und anschliessend vernichtet.

Art. 11

Aufgehoben

Art. 13 Bst. f und n–p

Das PISA dient zur Erfüllung folgender Aufgaben:

f. Durchführung der Erwerbsersatzordnung in der Armee oder im Zivilschutz;

n. Prüfung und Kontrolle der Ausbildungsgutschriften;

o. Fallführung im Rahmen der psychologischen Betreuung von Angehörigen der Armee während des Militärdienstes;

p. Verwendung seiner Daten in anonymisierter Form zur Beantwortung von Anfragen zu Zahlen betreffend das VBS.

Art. 14 Abs. 1 Bst. a^{bis}, c^{bis} und n, Abs. 2 Einleitungssatz und Abs. 4

1 Das PISA enthält folgende Daten der Stellungspflichtigen, der Militärdienstpflichtigen, des für die Friedensförderung vorgesehenen Personals sowie von Zivilpersonen, die von der Truppe betreut oder für einen befristeten Einsatz der Armee beigezogen werden:

a^{bis}. die bei der Rekrutierung mittels Untersuchungen, Tests und Befragungen erhobenen und als Grundlage für die Entscheide nach Buchstabe a dienenden Daten über:

1. den Gesundheitszustand: Anamnese, Elektrokardiogramm, Lungenfunktion, Hör- und Sehvermögen, Intelligenztest, Textverständnistest, Fragebogen zur Erkennung von psychischen Erkrankungen, freiwillige Labor- und Röntgenuntersuchungen,
2. die körperliche Leistungsfähigkeit: Kondition mit ihren Komponenten Ausdauer, Kraft, Schnelligkeit sowie koordinative Fähigkeiten,
3. die Intelligenz und Persönlichkeit: allgemeine Intelligenz, Problemlösefähigkeit, Konzentrationsfähigkeit und Aufmerksamkeit, Flexibilität, Gewissenhaftigkeit und Selbstbewusstsein sowie Veranlagung zu Handlungen,
4. die Psyche: Angstfreiheit, Selbstbewusstsein, Stressresistenz, emotionale Stabilität und Umgänglichkeit,
5. die soziale Kompetenz: Verhalten und Sensitivität in der Gesellschaft, der Gemeinschaft und der Gruppe,
6. die Eignung zur Ausübung bestimmter Funktionen: funktionsbezogene Eignungsprüfungen, soweit sich die Eignung nicht aus dem Leistungsprofil nach den Ziffern 1–5 ergibt,
7. das grundsätzliche Kaderpotenzial: Potenzial zur Verwendung als Unteroffizier, höherer Unteroffizier oder Offizier,

8. die persönlichen Interessen betreffend Erfüllung der Militärdienstpflicht,
9. das Gefahrenpotenzial betreffend den Missbrauch der persönlichen Waffe;

c^bis. Daten über absolvierte Ausbildungen und erlangte Berechtigungen für die Bedienung von militärischen Systemen;

n. Daten für die Prüfung und Kontrolle von Anträgen auf Auszahlung von Ausbildungsgutschriften.

2 Es enthält folgende Daten der Zivildienstpflichtigen:

4 Es enthält folgende Daten der vom psychologisch-pädagogischen Dienst der Armee (PPD) betreuten Personen:

a. Daten über Einteilung, Grad, Funktion und Ausbildung in der Armee;

b. folgende psychologische Daten:
   1. Daten zum psychischen Zustand,
   2. anamnestisch-biografisch erhobene Daten zu den psychischen Eigenschaften,
   3. Resultate psychologischer Tests,
   4. Zeugnisse von zivilen psychologischen Fachpersonen;

c. sanitätsdienstliche Daten psychologischer oder psychiatrischer Herkunft, die zur Erfüllung der Aufgaben nach Artikel 13 notwendig sind;

d. Korrespondenz mit den betreuten Personen sowie den involvierten Stellen;

e. Daten, die von der betreuten Person freiwillig gemeldet wurden.

Art. 15 Abs. 1 Einleitungssatz, Abs. 2 Bst. a und Abs. 4

1 Die Gruppe Verteidigung, die Kreiskommandantinnen und Kreiskommandanten und die für den Zivilschutz zuständigen Stellen von Bund und Kantonen beschaffen die Daten für das PISA bei:

2 Das PISA kann mit folgenden Informationssystemen von Bund und Kantonen so verbunden werden, dass die zuständigen Stellen und Personen diejenigen Daten, die in beiden Systemen geführt werden dürfen, von einem System ins andere übertragen können:

a. Veranstaltungsadministratorsystem (Art. 93 Abs. 2 des Bevölkerungs- und Zivilschutzgesetzes vom 20. Dezember 2019[6]; BZG);

4 Der PPD beschafft die Daten nach Artikel 14 Absatz 4 bei:

a. der von ihm betreuten Person;

b. den militärischen Vorgesetzten der betreuten Person;

c. dem Militärärztlichen Dienst;

d. Dritten, soweit die betreute Person dazu ihre Einwilligung gibt.

6 SR **520.1**

*Art. 16 Abs. 1 Einleitungssatz, Bst. b^bis^, h und i sowie Abs. 1^ter^*

[1] Die Gruppe Verteidigung macht die Daten des PISA, ausgenommen die Daten nach Artikel 14 Absatz 4, durch Abrufverfahren folgenden Stellen und Personen zugänglich, soweit diese die Daten zur Erfüllung ihrer gesetzlichen oder vertraglichen Aufgaben benötigen:

b^bis^. den mit der Rekrutierung beauftragten Stellen und Personen;

h. der Zentralen Ausgleichsstelle zur Durchführung der Erwerbsersatzordnung;

i. dem Nachrichtendienst des Bundes zur Feststellung der Identität von Personen, die aufgrund von Erkenntnissen über Bedrohungen für die innere oder äussere Sicherheit nach Artikel 6 Absatz 1 Buchstabe a des Nachrichtendienstgesetzes vom 25. September 2015[7] (NDG) eine Bedrohung für die Sicherheit der Armee darstellen können;

[1ter] Der PPD macht die Daten nach Artikel 14 Absatz 4 durch Abrufverfahren folgenden Stellen und Personen zugänglich:

a. den für die psychologische Betreuung der Angehörigen der Armee zuständigen Fachkräften des PPD;

b. den mit der Rekrutierung beauftragten Stellen, Ärztinnen und Ärzte;

c. den für den Militärärztlichen Dienst der Armee zuständigen Stellen.

Art. 17 Abs. 1 Bst. e und Abs. 4^ter^, 4^quater^ und 5

[1] Daten des PISA über Straftaten sowie strafrechtliche Entscheide und Massnahmen dürfen nur aufbewahrt werden, wenn gestützt auf diese Daten:

e. ein Entscheid über den Ausschluss aus dem Zivilschutz nach dem BZG[8] erging.

[4ter] Die Daten nach Artikel 14 Absatz 1 Buchstabe a^bis^, die zugleich sanitätsdienstliche Daten nach Artikel 26 Absatz 2 sind, werden nach Abschluss der Rekrutierung bis zur Bekanntgabe an das Medizinische Informationssystem der Armee (MEDISA), längstens aber während einer Woche aufbewahrt.

[4quater] Daten nach Artikel 14 Absatz 4 werden nach Abschluss der Betreuung längstens während fünf Jahren aufbewahrt.

[5] Die übrigen Daten des PISA werden nach der Entlassung aus der Militärdienst- oder Schutzdienstpflicht längstens während fünf Jahren aufbewahrt.

2. Kapitel 2. Abschnitt (Art. 18–23)

Aufgehoben

7 SR **121**
8 SR **520.1**

Art. 24 Verantwortliches Organ

Die Gruppe Verteidigung betreibt das Medizinische Informationssystem der Armee (MEDISA).

Art. 27 Einleitungssatz

Die Gruppe Verteidigung beschafft die Daten für das MEDISA bei:

Art. 28 Abs. 1 Einleitungssatz und Bst. c sowie Abs. 3 Einleitungssatz

1 Die Gruppe Verteidigung macht die Daten des MEDISA durch Abrufverfahren folgenden Stellen und Personen zugänglich:

c. den für die psychologische Betreuung der Angehörigen der Armee zuständigen Fachkräften des PPD;

3 Die Gruppe Verteidigung gibt die Entscheide über die Tauglichkeit für den Militär- und Schutzdienst folgenden Stellen bekannt:

Art. 30 Verantwortliches Organ

Die Gruppe Verteidigung betreibt dezentral auf den Waffenplätzen und in den Militärspitälern je ein Informationssystem Patientenerfassung (ISPE).

Art. 33 Einleitungssatz

Die Gruppe Verteidigung beschafft die Daten für die ISPE bei:

2. Kapitel 5. Abschnitt (Art. 36–41)

Aufgehoben

Art. 42 Verantwortliches Organ

Die Gruppe Verteidigung betreibt das Informationssystem Flugmedizin (MEDIS LW).

Art. 45 Einleitungssatz

Die Gruppe Verteidigung beschafft die Daten für das MEDIS LW bei:

Art. 46 Abs. 1 Einleitungssatz und Abs. 2

1 Die Gruppe Verteidigung macht die Daten des MEDIS LW durch Abrufverfahren folgenden Personen zugänglich, soweit diese die Daten zur Wahrnehmung ihrer gesetzlichen Aufgaben benötigen:

2 Sie gewährt in Anwesenheit eines Arztes, einer Ärztin, eines Psychologen oder einer Psychologin des Fliegerärztlichen Instituts den behandelnden und begutachtenden

Ärztinnen und Ärzten und denjenigen der Militärversicherung Einsicht in die Daten des MEDIS LW.

Art. 47 Abs. 1 und 3

[1] *Aufgehoben*

[3] Ist bei Ablauf der Aufbewahrungsdauer nach Absatz 2 eine Person noch in Behandlung oder Betreuung durch das Fliegerärztliche Institut, so werden ihre Daten nach Abschluss der Behandlung oder Betreuung während zehn Jahren aufbewahrt.

Gliederungstitel vor Art. 48

7. Abschnitt: Informationssystem Einsatzpersonal Kommando Spezialkräfte

Art. 48 Verantwortliches Organ

Die Gruppe Verteidigung betreibt das Informationssystem Einsatzpersonal Kommando Spezialkräfte (ISEP KSK).

Art. 49 Zweck

Das ISEP KSK dient:

a. der psychologisch-psychiatrischen und medizinischen Evaluation der Anwärterinnen und Anwärter für das Armee-Aufklärungsdetachement und das Militärpolizei-Spezialdetachement;

b. der einsatzbezogenen Evaluation der Angehörigen des Armee-Aufklärungsdetachements und des Militärpolizei-Spezialdetachements;

c. *Betrifft nur den französischen Text.*

Art. 50 Daten

Das ISEP KSK enthält die für die Evaluation und die Beurteilung der Einsatzfähigkeit mittels Untersuchungen, Tests und Befragungen erhobenen Daten zur biostatistischen Einschätzung des Ausfallrisikos beziehungsweise des Durchhaltevermögens im Einsatz.

Art. 51 Einleitungssatz

Die Gruppe Verteidigung beschafft die Daten für das ISEP KSK bei:

Art. 52 Abs. 1

[1] Die Gruppe Verteidigung macht die Daten des ISEP KSK den mit der Evaluation beauftragten Psychologinnen und Psychologen sowie der Ärztin oder dem Arzt Sonderoperationen durch Abrufverfahren zugänglich.

Art. 53 Abs. 2

[2] Die Daten der Angehörigen des Armee-Aufklärungsdetachements, der Angehörigen des Militärpolizei-Spezialdetachements sowie derjenigen Personen des Kommandos Spezialkräfte, die zur Einsatzunterstützung eingesetzt werden, werden bis zum Ausscheiden aus dem Detachement beziehungsweise dem Kommando Spezialkräfte aufbewahrt.

Gliederungstitel vor Art. 54

8. Abschnitt: Informationssystem für die soziale Beratung

Art. 54 Verantwortliches Organ

Die Gruppe Verteidigung betreibt ein Informationssystem für die soziale Beratung (ISB).

Art. 55 Zweck

Das ISB dient der administrativen Unterstützung der sozialen Beratung und Betreuung von Angehörigen der Armee, Angehörigen des Zivilschutzes, Angehörigen des Rotkreuzdienstes, Personen im Friedensförderungsdienst, Angehörigen der Militärjustiz, Militärpatientinnen und Militärpatienten sowie von Angehörigen und Hinterbliebenen der vorgenannten Personen.

Art. 56 Daten

Das ISB enthält Angaben zur geleisteten finanziellen Unterstützung und zur Fallführung, Notizen zur Gesprächsführung sowie persönliche Unterlagen und Dokumente, die für die Beurteilung einer sozialen Beratung und Betreuung notwendig sind.

Art. 57 Datenbeschaffung

Die Gruppe Verteidigung beschafft die Daten für das ISB:

a. bei der betreffenden Person oder ihrer gesetzlichen Vertretung;
b. bei den militärischen Kommandos;
c. bei den zuständigen Verwaltungseinheiten des Bundes und der Kantone;
d. bei den von der betreffenden Person genannten Referenzpersonen;
e. aus dem PISA.

Art. 58 Datenbekanntgabe

Die Gruppe Verteidigung macht die Daten des ISB durch Abrufverfahren folgenden Stellen und Personen zugänglich:

a. den Mitarbeitenden des Sozialdienstes der Armee;

b. den Angehörigen der Armee, die beim Fachstab des Sozialdienstes der Armee eingeteilt sind;
c. der Fachstelle Diversity Schweizer Armee die Daten zu deren Klientinnen und Klienten;
d. der Armeeseelsorge die Daten zu deren Klientinnen und Klienten.

Art. 63 Abs. 2

2 Die Daten nach Artikel 62, die im Informationssystem für das Personaldatenmanagement (IPDM) enthalten sind, werden dem IPV durch Abrufverfahren zugänglich gemacht.

Art. 65 Abs. 2

2 Die Daten von Kandidatinnen und Kandidaten, die nicht angestellt wurden, werden spätestens nach sechs Monaten vernichtet.

Art. 72 Verantwortliches Organ

Die Gruppe Verteidigung betreibt ein Informations- und Einsatz-System Koordinierter Sanitätsdienst (IES-KSD).

Art. 73 Einleitungssatz

Das IES-KSD dient der oder dem Beauftragten des Bundesrates für den Koordinierten Sanitätsdienst (KSD) sowie den zivilen und militärischen Stellen, die mit der Planung, Vorbereitung und Durchführung von sanitätsdienstlichen Massnahmen beauftragt sind (KSD-Partnern), bei der Bewältigung von sanitätsdienstlich relevanten Ereignissen für folgende Aufgaben:

Art. 75 Einleitungssatz

Die oder der Beauftragte des Bundesrates für den KSD sowie die KSD-Partner beschaffen die Daten für das IES-KSD bei:

Art. 85 Abs. 2

2 Es dient zudem der Durchführung der Erwerbsersatzordnung.

Art. 86 Bst. a, a^{bis} und h

Das MIL Office enthält folgende Daten:

a. Personalien, Adresse und Kontaktangaben;
a^{bis}. Daten über Einteilung, Grad, Funktion und Ausbildung;
h. Daten für die Verwaltung und Zuweisung von Armeematerial.

Art. 87 Bst. a

Die militärischen Kommandos beschaffen die Daten für das MIL Office:

a. bei der betreffenden Person; diese kann die Daten auch freiwillig über ein von der Gruppe Verteidigung betriebenes elektronisches Portal übermitteln.

Art. 88 Datenbekanntgabe

Die militärischen Kommandos geben die Daten des MIL Office folgenden Stellen und Personen bekannt:

a. *Betrifft nur den französischen Text.*

b. *Betrifft nur den französischen Text.*

c. *Betrifft nur den französischen Text.*

d. der Zentralen Ausgleichsstelle zur Durchführung der Erwerbsersatzordnung: die Daten nach Artikel 86 Buchstaben a, a^{bis}, c und g.

Art. 94 Datenbekanntgabe

Das Generalsekretariat des VBS macht die Daten des ISKM den für die Kaderplanung und -entwicklung sowie das Kompetenzmanagement zuständigen Stellen und Personen des VBS, der betreffenden Person und ihren Vorgesetzten durch Abrufverfahren zugänglich.

Art. 103 Einleitungssatz sowie Bst. a und c

Das FIS HE dient der Gruppe Verteidigung und den militärischen Kommandos zur Erfüllung folgender Aufgaben:

a. Aktionsplanung und Lageverfolgung der Stäbe und Verbände des Kommandos Operationen und der Führungsunterstützungsbasis;

c. Vernetzung von Aufklärungs-, Führungs- und Einsatzmitteln des Kommandos Operationen und der Führungsunterstützungsbasis.

Art. 109 Bst. a

Das FIS LW dient der Luftwaffe und ihren militärischen Kommandos zur Erfüllung folgender Aufgaben:

a. Aktionsplanung und Lageverfolgung der Stäbe und Verbände der Luftwaffe;

Art. 110 Bst. a

Das FIS LW enthält die folgenden Daten der Angehörigen der Armee:

a. Geschlecht;

Art. 119 Datenaufbewahrung

Die Daten des IMESS werden nach Beendigung des Einsatzes vernichtet.

Art. 121 Zweck

Die Informationssysteme von Simulatoren dienen zur Unterstützung der Ausbildung und Qualifikation von:

a. Angehörigen der Armee;

b. Zivilpersonen, die für einen befristeten Einsatz der Armee beigezogen werden;

c. Dritten, die an den Simulatoren trainieren.

Art. 123 Einleitungssatz und Bst. c

Die zuständigen Stellen und Personen beschaffen die Daten für die Informationssysteme von Simulatoren bei:

c. den militärischen oder zivilen Vorgesetzten der betreffenden Person.

Art. 124 Abs. 2 Bst. c

2 Sie geben die Daten der Informationssysteme von Simulatoren bekannt:

c. den an den Simulatoren ausgebildeten Zivilpersonen oder trainierenden Dritten sowie deren vorgesetzten Stellen und Personen.

Art. 125 Abs. 2

2 Trainieren Angehörige der Armee, Zivilpersonen oder Dritte regelmässig auf denselben Simulatoren, so können die Daten der Trainings nach deren Abschluss jeweils während zehn Jahren aufbewahrt werden.

Art. 131 Datenaufbewahrung

Die Daten des LMS VBS werden längstens während zehn Jahren aufbewahrt:

a. nach Entlassung der Angehörigen der Armee aus der Militärdienstpflicht;

b. nach Beendigung des Arbeitsverhältnisses der Angestellten des VBS.

Gliederungstitel vor Art. 138

4. Abschnitt: Informationssystem Strassenverkehr und Schifffahrt der Armee

Art. 138 Verantwortliches Organ

Die Gruppe Verteidigung betreibt das Informationssystem Strassenverkehr und Schifffahrt der Armee (FA-SVSAA).

Art. 139 Einleitungssatz sowie Bst. a, c, e und f

Das FA-SVSAA dient:

a. der Erstellung und Verwaltung von militärischen Fahrberechtigungen für Fahrzeug- und Schiffsführerinnen und -führer, von eidgenössischen Schiffsführerausweisen sowie von Ausweisen der militärischen Verkehrsexpertinnen und -experten;

c. der Umsetzung von Administrativmassnahmen in Bezug auf militärische Fahrzeug- und Schiffsführerinnen und -führer, Inhaberinnen und Inhaber eidgenössischer Schiffsführerausweise sowie militärische Verkehrsexpertinnen und -experten;

e. der Kontrolle der Ausbildung der angehenden Fahrerinnen und Fahrer, der Armeefahrlehrerinnen und -lehrer sowie der militärischen Verkehrsexpertinnen und -experten;

f. *Aufgehoben*

Art. 140 Einleitungssatz und Bst. b–d

Das FA-SVSAA enthält folgende Daten von angehenden Fahrerinnen und Fahrern, von Fahrberechtigten, von Armeefahrlehrerinnen und -lehrern sowie von militärischen Verkehrsexpertinnen und -experten:

b. Daten über die Ausbildung, die militärischen Fahrberechtigungen und die Ausweise;

c. Daten über die Administrativmassnahmen;

d. Daten über die Ergebnisse der letzten Kontrolluntersuchung und das Datum der nächsten Kontrolluntersuchung.

Art. 141 Einleitungssatz und Bst. b–e

Die Gruppe Verteidigung beschafft die Daten für das FA-SVSAA:

b. aus dem Informationssystem Verkehrszulassung (IVZ) des Bundesamts für Strassen;

c. aus dem IPV;

d. aus dem IPDM;

e. bei den Stellen und Personen, die mit den Aufgaben nach Artikel 139 betraut sind.

Art. 142 Abs. 1

1 Die Gruppe Verteidigung gibt die Daten des FA-SVSAA bekannt:

a. den Stellen und Personen, die mit den Aufgaben nach Artikel 139 betraut sind;

b. an das PISA und das IVZ.

Art. 143 Datenaufbewahrung

[1] Die Daten des FA-SVSAA, einschliesslich Daten über militärische Administrativmassnahmen des Strassenverkehrs- und Schifffahrtsamts der Armee, werden nach der Erfassung längstens während 80 Jahren aufbewahrt.

[2] Die Daten über zivile Administrativmassnahmen werden längstens so lange aufbewahrt, wie sie im IVZ enthalten sind.

[3] Die Daten über eine Kontrolluntersuchung werden jeweils nur bis zur nächsten Kontrolluntersuchung aufbewahrt.

Art. 143c Bst. l

Das SPHAIR-Expert enthält folgende Daten:

l. persönliche Interessen hinsichtlich der Anstellung, Ausbildung, Weiterentwicklung sowie Berufs- und Funktionswahl.

6. Abschnitt (Art. 143g–143l) einfügen vor dem Gliederungstitel des 5. Kapitels

6. Abschnitt: Informationssystem Führungsausbildung

Art. 143g Verantwortliches Organ

Die Gruppe Verteidigung betreibt das Informationssystem Führungsausbildung (ISFA).

Art. 143h Zweck

Das ISFA dient der Ausbildungskontrolle, der Analyse der Ausbildungsresultate und der Prüfungsorganisation.

Art. 143i Daten

Das ISFA enthält folgende Daten:

a. Personalien, Wohnort, Heimatort, Heimatkanton und Adressen;

b. Daten über Einteilung, Grad, Funktion und Dienstleistungen in der Armee;

c. AHV-Nummer;

d. Geschlecht;

e. Geburtsdatum;

f. ausbildungs- und prüfungsbezogene Daten, Kandidatinnen- oder Kandidatennummer, Prüfungssprache und Prüfungsangaben (Datum, Zeit, Ort, Expertin oder Experte);

g. Daten über Eigenleistungen (Einreichdatum, Ergebnis);

h. Prüfungsteilnahme und Prüfungsergebnisse.

Art. 143j Datenbeschaffung

Die Gruppe Verteidigung beschafft die Daten für das ISFA:

a. bei der betreffenden Person;

b. bei den militärischen Vorgesetzten der betreffenden Person;

c. bei den zuständigen Verwaltungseinheiten der Gruppe Verteidigung;

d. aus dem PISA.

Art. 143k Datenbekanntgabe

1 Die Gruppe Verteidigung macht die Daten des ISFA durch Abrufverfahren den Stellen und Personen zugänglich:

a. die für die Eingabe der Daten in das ISFA zuständig sind;

b. die für die Koordination der Prüfungen für die einzelnen Module zuständig sind.

2 Die Daten des ISFA werden bekannt gegeben:

a. der für die Ausstellung des Zertifikats über die erfolgreiche Absolvierung der einzelnen Module zuständigen zivilen Stelle;

b. den im ISFA erfassten Personen als persönlicher Ausbildungsnachweis.

Art. 143l Datenaufbewahrung

Die Daten des ISFA werden nach der Erfassung längstens während zehn Jahren aufbewahrt.

Art. 145 Zweck

Das SIBAD dient der Durchführung von:

a. Personensicherheitsprüfungen;

b. Beurteilungen des Gefährdungs- oder Missbrauchspotenzials bezüglich der persönlichen Waffe;

c. Zuverlässigkeitskontrollen.

Art. 147 Abs. 2 Einleitungssatz sowie Bst. c und d

2 Sie haben durch Abrufverfahren Zugang zu folgenden Registern und Datenbanken im Rahmen der entsprechenden Rechtsgrundlagen:

c. Informationssystem INDEX NDB nach Artikel 51 NDG[9], unter Vorbehalt von Artikel 20 Absatz 2 des Bundesgesetzes vom 21. März 1997[10] über Massnahmen zur Wahrung der inneren Sicherheit;

9 SR **121**
10 SR **120**

d. Datenbanken der Zentralstelle Waffen nach Artikel 32*a* Absatz 1 WG[11].

Art. 148 Abs. 1 Einleitungssatz sowie Bst. c Ziff. 2bis und Bst. d

1 Die Fachstelle PSP VBS macht die Daten des SIBAD durch Abrufverfahren folgenden Stellen zugänglich:

c. den mit der Einleitung der Personensicherheitsprüfungen beauftragten Stellen:
   2bis. der nationalen Netzgesellschaft,

d. den mit Sicherheitsaufgaben beauftragten Stellen des Bundes, wenn diese Stellen sich für ihre Tätigkeit auf die Daten der Personensicherheitsprüfungen stützen müssen und die Daten für die betreffende Person nicht nachteilig sind.

Gliederungstitel vor Art. 167a

5. Abschnitt: Journal- und Rapportsystem der Militärpolizei

Art. 167a Verantwortliches Organ

Die Gruppe Verteidigung betreibt ein Journal- und Rapportsystem der Militärpolizei (JORASYS).

Art. 167b Bst. a und b

Betrifft nur den französischen Text.

Art. 167d Datenbeschaffung

Das Kommando Militärpolizei beschafft die Daten für das JORASYS:

a. bei der betreffenden Person;

b. bei den militärischen Kommandos;

c. bei den zuständigen Verwaltungseinheiten von Bund, Kantonen und Gemeinden;

d. bei den zivilen und militärischen Straf-, Strafvollzugs- und Verwaltungsrechtspflegebehörden;

e. durch Abrufverfahren oder automatisiert über eine Schnittstelle aus:
   1. dem nationalen Polizeiindex,
   2. dem automatisierten Polizeifahndungssystem RIPOL des Bundesamtes für Polizei,
   3. dem IVZ,
   4. den Datenbanken der Zentralstelle Waffen nach Artikel 32*a* Absatz 1 WG[12],

11 SR **514.54**
12 SR **514.54**

5. der Online-Abfrage Waffenregister der Kantone,
6. dem PISA,
7. dem IPV,
8. dem FA-SVSAA,
9. dem Informationssystem Datendrehscheibe Verteidigung (DDSV),
10. dem PSN.

Art. 167e Abs. 1 und 2 Bst. b und c

[1] Das Kommando Militärpolizei macht die Daten des JORASYS durch Abrufverfahren folgenden Personen zugänglich:

a. *Betrifft nur den französischen Text.*

b. den Mitarbeiterinnen und Mitarbeitern des Kommandos Militärpolizei für die Erfüllung ihrer Aufgaben nach Artikel 100 MG[13];

c. den Mitarbeiterinnen und Mitarbeitern des Dienstes für präventiven Schutz der Armee (DPSA) für die Erfüllung ihrer Aufgaben nach Artikel 100 MG.

[2] Es gibt die Daten des JORASYS in Form schriftlicher Auszüge folgenden Stellen und Personen bekannt:

b. den zuständigen Truppenkommandantinnen und Truppenkommandanten für ihren Bereich;

c. den für die Informations- und Objektsicherheit zuständigen Stellen.

Art. 167f Datenaufbewahrung

Die Daten des JORASYS werden nach Abschluss der militärpolizeilichen Tätigkeit zu einem Vorfall während zehn Jahren aufbewahrt.

6. Abschnitt (Art. 167g–167l) einfügen vor dem Gliederungstitel des 6. Kapitels

6. Abschnitt: Informationssystem Präventiver Schutz der Armee

Art. 167g Verantwortliches Organ

Die Gruppe Verteidigung betreibt das Informationssystem Präventiver Schutz der Armee (IPSA).

Art. 167h Zweck

Das IPSA dient dem DPSA zur Erfüllung der Aufgaben nach Artikel 100 Absatz 1 MG[14], insbesondere:

a. zur Beurteilung der militärischen Sicherheitslage;

13 SR **510.10**
14 SR **510.10**

b. zum vorsorglichen Schutz vor Spionage, Sabotage und weiteren rechtswidrigen Handlungen;

c. zur Journal- und Einsatzführung.

Art. 167i Daten

Das IPSA enthält von Personen, von denen eine mögliche Bedrohung der Armee ausgeht, folgende Daten:

a. Personalien;

b. Zivilstand, Geburts- und Heimatort sowie Beruf und Ausbildung;

c. Staatsangehörigkeit, ethnische und religiöse Zugehörigkeit, Aufenthaltsstatus;

d. Daten zum Nachweis der Identität, einschliesslich körperlicher Merkmale;

e. politische und ideologische Ausrichtung;

f. Rekrutierungsergebnisse, Einteilung, Grad, Funktion, Ausbildung, Qualifikationen, Dienstleistungen, Einsätze und Ausrüstung in der Armee und im Zivilschutz;

g. Einkommens- und Vermögensverhältnisse;

h. medizinische und biometrische Daten;

i. Bild-, Film- und Tonaufnahmen;

j. Bezugspersonen sowie deren Identität;

k. Daten über den Aufenthaltsort der Person, einschliesslich Bewegungsprofilen;

l. Daten über die von der Person verwendeten Fortbewegungs- und Kommunikationsmittel, einschliesslich Nutzungs- und Standortdaten sowie Bewegungsprofilen;

m. Einzelheiten zu der von einer Person ausgehenden möglichen Bedrohung der Armee;

n. weitere Informationen und Daten, die der DPSA für die Erfüllung der Aufgaben nach Artikel 100 Absatz 1 MG[15] benötigt.

Art. 167j Datenbeschaffung

Der DPSA beschafft die Daten für das IPSA:

a. bei der betreffenden Person;

b. bei den militärischen Kommandos;

c. bei den in- und ausländischen Nachrichtendiensten;

d. bei den Verwaltungseinheiten von Bund, Kantonen und Gemeinden;

15 SR **510.10**

e. bei den zivilen und militärischen Strafbehörden sowie den Verwaltungsrechtspflegebehörden;

f. aus öffentlich zugänglichen Quellen;

g. durch Abrufverfahren aus dem:
   1. PISA,
   2. FA-SVSAA,
   3. JORASYS,
   4. DDSV,
   5. PSN.

Art. 167k Datenbekanntgabe

[1] Der DPSA macht die Daten des IPSA durch Abrufverfahren seinen Mitarbeiterinnen und Mitarbeitern für die Erfüllung ihrer Aufgaben nach Artikel 100 MG[16] zugänglich.

[2] Er gibt die Daten des IPSA in Form schriftlicher Auszüge folgenden Stellen und Personen bekannt, soweit diese die Daten zur Erfüllung ihrer gesetzlichen Aufgaben benötigen:

a. den für die Informations- und Objektsicherheit zuständigen Stellen;

b. den für die Cyberabwehr zuständigen Stellen;

c. der Fachstelle Extremismus in der Armee;

d. dem Kommando Militärpolizei;

e. der Organisationseinheit Personelles der Armee;

f. den zuständigen Truppenkommandantinnen und Truppenkommandanten für ihren Bereich;

g. dem Nachrichtendienst des Bundes; vorbehalten bleibt Artikel 5 Absatz 5 NDG[17];

h. dem Bundesamt für Polizei.

Art. 167l Datenaufbewahrung

Die Daten des IPSA werden nach dem Wegfall der von der betreffenden Person ausgehenden möglichen Bedrohung der Armee längstens während fünf Jahren aufbewahrt.

Gliederungstitel vor Art. 168

Betrifft nur den französischen und den italienischen Text.

16 SR **510.10**
17 SR **121**

Art. 168 Verantwortliches Organ

Das Generalsekretariat des VBS betreibt ein Informationssystem Schadenzentrum VBS (SCHAMIS).

Art. 169 Einleitungssatz sowie Bst. d und e

Das SCHAMIS dient:

d. dem Ausstellen von elektronischen Versicherungsnachweisen für Bundesfahrzeuge;

e. der Regulierung von Schadenfällen von Motorfahrzeugen von Ratsmitgliedern nach Artikel 4 Absatz 2 der Verordnung der Bundesversammlung vom 18. März 1988[18] zum Parlamentsressourcengesetz.

Art. 170 Einleitungssatz sowie Bst. a und a^{bis}

Das SCHAMIS enthält:

a. folgende Daten von Geschädigten und Schädigenden:
   1. Personalien, Adresse, Kontaktangaben und Korrespondenzsprache,
   2. Sozialversicherungsnummer,
   3. Angaben zur finanziellen und beruflichen Situation,
   4. Daten von Versicherungen,
   5. medizinische und sanitätsdienstliche Daten,
   6. Daten aus Straf-, Zivil-, Disziplinar- und Verwaltungsverfahren,
   7. militärische Führungsdaten,
   8. Fahrzeughalterdaten;

a^{bis}. folgende für die Zweckerfüllung nötigen Daten von Dritten:
   1. Personalien, Adresse, Kontaktangaben und Korrespondenzsprache,
   2. Beruf;

Art. 171 Einleitungssatz und Bst. i

Das Generalsekretariat des VBS beschafft die Daten für das SCHAMIS bei:

i. Versicherungen.

Art. 172 Datenbekanntgabe

[1] Das Generalsekretariat des VBS macht die Daten des SCHAMIS den mit den Aufgaben nach Artikel 169 betrauten Mitarbeiterinnen und Mitarbeitern durch Abrufverfahren zugänglich.

[2] Es gibt Dritten, die bei der Erledigung von Schadenfällen und Haftpflichtansprüchen mitwirken, die dafür notwendigen Daten bekannt.

[18] SR **171.211**

Art. 173 Datenaufbewahrung

Die Daten des SCHAMIS werden nach dem rechtskräftigen Abschluss des Verfahrens während zehn Jahren aufbewahrt.

Gliederungstitel vor Art. 174

2. Abschnitt: Informationssystem Datendrehscheibe Verteidigung

Art. 174 Verantwortliches Organ

Die Gruppe Verteidigung betreibt das Informationssystem Datendrehscheibe Verteidigung (DDSV).

Art. 175 Einleitungssatz

Das DDSV dient zur Erfüllung folgender Aufgaben:

Art. 176 Einleitungssatz und Bst. c

Das DDSV enthält folgende Daten:

c. Daten, die für den Datenaustausch nach Artikel 175 Buchstabe c notwendig sind.

Art. 177 Einleitungssatz

Die Gruppe Verteidigung beschafft die Daten für das DDSV bei:

Art. 178 Datenbekanntgabe

Die Gruppe Verteidigung macht durch Abrufverfahren die folgenden Daten des DDSV den nachstehenden Stellen und Personen zugänglich:

a. die Daten nach Artikel 176 Buchstaben a und b: den militärischen Kommandos sowie den zuständigen Verwaltungseinheiten des Bundes und der Kantone;

b. die Daten nach Artikel 176 Buchstabe c: den für die militärischen Informationssysteme zuständigen Stellen und Personen.

Art. 179 Datenaufbewahrung

Die Daten des DDSV werden längstens während fünf Jahren aufbewahrt.

Art. 179b Bst. d

Das PSN dient der logistischen, personellen und finanziellen Führung der Armee und der Verwaltungseinheiten der Gruppe Verteidigung; es bezweckt:

d. den Austausch von Daten mit der Datenbank nach Artikel 32*a* Absatz 1 Buchstabe d WG[19];

Art. 179c Abs. 4

4 Es enthält die Daten der Stellenbewerberinnen und Stellenbewerber sowie Angestellten aus den gestützt auf das BPG[20] und dessen Ausführungsbestimmungen geführten Bewerbungs- und Personaldossiers.

Art. 179d Bst. e

Die Verwaltungseinheiten der Gruppe Verteidigung beschaffen die Daten für das PSN bei:

e. den zuständigen Verwaltungseinheiten des Bundes und der Kantone aus den militärischen Informationssystemen, dem IPDM und der Datenbank nach Artikel 32*a* Absatz 1 Buchstabe c WG[21].

Art. 179e Abs. 2 Bst. e

2 Sie geben die Daten des PSN zur Erfüllung ihrer gesetzlichen oder vertraglichen Aufgaben bekannt:

e. den Verwaltungseinheiten der Bundesverwaltung über eine Schnittstelle mit dem IPDM;

Gliederungstitel vor Art. 179g

4. Abschnitt: Informationssystem Schiesswesen ausser Dienst

Art. 179g Verantwortliches Organ

Die Gruppe Verteidigung betreibt das Informationssystem Schiesswesen ausser Dienst (SaD).

Art. 179h Einleitungssatz

Das SaD dient der Verwaltung und dem Betrieb des Schiesswesens ausser Dienst bei:

Art. 179i Einleitungssatz

Das SaD enthält folgende für die Kontrolle von obligatorischen Schiessen und anderen Schiessen im Interesse der Landesverteidigung benötigten Daten von schiesspflichtigen Angehörigen der Armee, von Funktionärinnen und Funktionären im Schiesswesen ausser Dienst, von anerkannten Schiessvereinen und deren Mitgliedern sowie von Schützinnen und Schützen:

19 SR **514.54**
20 SR **172.220.1**
21 SR **514.54**

Art. 179j Einleitungssatz

Die Gruppe Verteidigung beschafft die Daten für das SaD bei:

Art. 179k Abs. 1 Einleitungssatz und Abs. 2

[1] Die Gruppe Verteidigung macht die Daten des SaD durch Abrufverfahren folgenden Stellen und Personen für die Erfüllung ihrer Aufgaben zugänglich:

[2] Sie gibt die für die Abrechnung und die Kontrolle nach Artikel 179*h* notwendigen Daten des SaD der Alters- und Hinterlassenenversicherung, den Steuerverwaltungen und der mit dem Zahlungsverkehr betrauten Stelle bekannt.

Art. 179l Abs. 1

[1] Die Daten des SaD werden während fünf Jahren nach dem letzten Eintrag aufbewahrt.

5. Abschnitt (Art. 179m–179r) einfügen vor dem Gliederungstitel des 7. Kapitels

5. Abschnitt: Informationssystem Master-Data-Management

Art. 179m Verantwortliches Organ

Das Generalsekretariat des VBS betreibt das Informationssystem Master-Data-Management (MDM).

Art. 179n Zweck

Das MDM dient der Verwaltung und Bereitstellung von Daten bestehender und künftig möglicher Geschäftspartnerinnen und Geschäftspartner für die Geschäftsprozesse des VBS in den Bereichen Finanzen, Beschaffung, Logistik, Immobilien und Personal.

Art. 179o Daten

Das MDM enthält die folgenden Daten bestehender und künftig möglicher Geschäftspartnerinnen und Geschäftspartner:

a. Namens- und Firmendaten;
b. Adressdaten;
c. Kontoverbindung;
d. Kontaktangaben;
e. Geschlecht;
f. Nationalität;
g. Korrespondenzsprache;
h. Ausländerkategorie;

i. Beruf;

j. Geburtsdatum;

k. Sozialversicherungsnummer;

l. Rechtsform;

m. Unternehmensidentifikationsnummer (UID), Steuernummer sowie weitere, unternehmensspezifische Nummern und Einteilungscodes;

n. Konkursangaben;

o. Status als Geschäftspartnerin oder Geschäftspartner;

p. mit der Geschäftspartnerin oder dem Geschäftspartner verknüpfte logistische Stammdaten wie Materialstammdaten und Systemstrukturdaten.

Art. 179p Datenbeschaffung

Das Generalsekretariat des VBS beschafft die Daten für das MDM:

a. bei den bestehenden und künftig möglichen Geschäftspartnerinnen und Geschäftspartnern;

b. bei den Verwaltungseinheiten des Bundes, der Kantone und der Gemeinden;

c. aus dem für das Master-Data-Management ausserhalb des VBS betriebenen Informationssystem des Bundes über eine Schnittstelle;

d. bei in- und ausländischen Materiallieferanten und -herstellern.

Art. 179q Datenbekanntgabe

Das Generalsekretariat des VBS macht die Daten des MDM durch Abrufverfahren den für die Geschäftsprozesse des VBS in den Bereichen Finanzen, Beschaffung, Logistik, Immobilien und Personal zuständigen Stellen und Personen zugänglich.

Art. 179r Datenaufbewahrung

1 Die Daten des MDM werden nach Beendigung der Geschäftsbeziehung zu einer Geschäftspartnerin oder einem Geschäftspartner wie folgt aufbewahrt:

a. die Daten nach Artikel 179*o* Buchstaben a–o: während zehn Jahren;

b. die Daten nach Artikel 179*o* Buchstabe p: während fünfzig Jahren.

2 Steht fest, dass eine Person nicht Geschäftspartnerin oder Geschäftspartner wird, werden ihre Daten während zwei Jahren aufbewahrt.

Art. 181 Abs. 1 Bst. a und Abs. 2 Einleitungssatz

1 Die Überwachungsmittel dienen zur Erfüllung folgender Aufgaben:

a. Gewährleistung der Sicherheit von Angehörigen, Einrichtungen und Material der Armee im Bereich:

1. der Truppe,

2. militärisch genutzter Objekte der Armee, der Militärverwaltung oder von Dritten;

2 Die Armee kann mit ihren Überwachungsmitteln und dem nötigen Personal den zivilen Behörden auf Gesuch hin luftgestützte Überwachungsleistungen erbringen:

Art. 186 Abs. 3

3 Er kann im Rahmen der Aussen- und Sicherheitspolitik internationale Abkommen über die grenzüberschreitende Bearbeitung von Personendaten, deren Bearbeitung nach DSG[22] keine Grundlage in einem Gesetz im formellen Sinn erfordert, abschliessen.

II

Die nachstehenden Erlasse werden wie folgt geändert:

1. Militärgesetz vom 3. Februar 1995[23]

Art. 146 Militärische Informationssysteme

Die Bearbeitung von Personendaten in Informationssystemen und beim Einsatz von Überwachungsmitteln der Armee und der Militärverwaltung wird im Bundesgesetz vom 3. Oktober 2008[24] über militärische und andere Informationssysteme im VBS geregelt.

2. Informationssicherheitsgesetz vom 18. Dezember 2020[25]

Art. 45 Abs. 1, 3bis und 6 Bst. d

1 Die Fachstellen PSP betreiben ein Informationssystem. Dieses dient der Durchführung von:

a. Personensicherheitsprüfungen;

b. Beurteilungen des Gefährdungs- oder Missbrauchspotenzials bezüglich der persönlichen Waffe;

c. Zuverlässigkeitskontrollen;

d. Prüfungen der Vertrauenswürdigkeit.

3bis Anhand der Daten des Informationssystems darf ein Profiling, einschliesslich eines Profilings mit hohem Risiko, nach DSG durchgeführt werden, um die nachfolgenden

22 SR **235.1**
23 SR **510.10**
24 SR **510.91**
25 SR **…**; BBl **2020** 9975

persönlichen Aspekte einer natürlichen Person zu den Bearbeitungszwecken nach Absatz 1 zu analysieren, zu bewerten, zu beurteilen oder vorherzusagen:

a. Sicherheitsrisiko;

b. Gefährdungs- und Missbrauchspotenzial bezüglich der persönlichen Waffe.

6 Die Daten nach Absatz 4 können automatisch und systematisch durch Abfrage der folgenden Informationssysteme erhoben werden:

d. die Datenbanken der Zentralstelle Waffen nach Artikel 32*a* Absatz 1 des Waffengesetzes vom 20. Juni 1997[26].

III

1 Dieses Gesetz untersteht dem fakultativen Referendum.

2 Der Bundesrat bestimmt unter Vorbehalt der Absätze 3 und 4 das Inkrafttreten.

3 Artikel 2*b* tritt nicht vor dem Datenschutzgesetz vom 25. September 2020[27] in Kraft.

4 Artikel 45 Absatz 3bis des Informationssicherheitsgesetzes vom 18. Dezember 2020[28] tritt nicht vor dem Datenschutzgesetz vom 25. September 2020[29] in Kraft.

26 SR **514.54**
27 SR **…**; BBl **2020** 7639
28 SR **…**; BBl **2020** 9975
29 SR **…**; BBl **2020** 7639