Datenschutzkonzept der Universität der Bundeswehr München

Stand: 01. Juni 2016

Inhalt

Grundlagen/Bezugsdokumente

1. Bundesdatenschutzgesetz (BDSG) in der jeweils gültigen Fassung

2. Zentrale Dienstvorschrift A-2122/4 (Anwendung und Erläuterung des Bundesdatenschutzgesetzes im Geschäftsbereich des Bundesministeriums der Verteidigung)

3. Gesetz zur Regelung des Zugangs zu Informationen des Bundes (Informationsfreiheitsgesetz – IFG) vom 05. September 2005

4. Bundesbeamtengesetz (insbesondere §§ 106-115) vom 05. Februar 2009 (BGBl. I S. 160), zuletzt geändert durch Art. 2 des Gesetzes vom 03. Dezember 2015 (BGBl. I S. 2178)

5. Soldatengesetz (insbesondere § 29) in der Fassung der Bekanntmachung vom 30. Mai 2005 (BGBl. I S. 1482), zuletzt geändert durch Art. 6 des Gesetzes vom 03. Dezember 2015 (BGBl. I S. 2163)

6. Gesetz über die Statistik für Bundeszwecke (Bundesstatistikgesetz – BStatG) vom 22. Januar 1987 (BGBl. I S. 462, 565), zuletzt geändert durch Art. 13 des Gesetzes vom 25. Juli 2013 (BGBl. I S. 2749)

7. Gesetz über die Statistik für das Hochschulwesen sowie für die Berufsakademien (Hochschulstatistikgesetz – HStatG) vom 02. November 1990 (BGBl. I S. 2414), zuletzt geändert durch Art. 1 des Gesetzes vom 02. März 2016 (BGBl. I S. 342)

8. Zentrale Dienstvorschrift A-2645/1 (Telearbeit)

9. Richtlinie über die Einhaltung des Datenschutzes bei Evaluation von Studium und Lehre an der Universität der Bundeswehr München (RL/EvaO) vom 01. Juni 2012

10. Hinweise zur Erfassung aller automatisierten Verarbeitungen personenbezogener Daten im zentralen Melderegister DATAV

11. Anmeldung einer automatisierten Verarbeitung zum Melderegister DATAV (Muster)

12. Ausfüllhilfe zur Anmeldung einer automatisierten Verarbeitung zum Melderegister DATAV

13. Datenschutzerklärung des Rechenzentrums in der jeweils gültigen Fassung

14. Hinweise zur IT-Sicherheit vom 18. Februar 2016

15. Richtlinie: Mobilgeräte im Datennetz vom 07. August 2012

16. Datenschutzrechtliche Belehrung der Präsidentin vom 21. Dezember 2009

Alle Grundlagen und Bezugsdokumente sind im Intranet UniBwM abrufbar (vgl. Nr. 13)

1. Zweckbestimmung

Dieses Konzept regelt Eckpunkte und Abläufe sowie Verantwortlichkeiten für alle Angehörigen der Universität der Bundeswehr München (UniBwM) beim Umgang mit personenbezogenen Daten.

2. Informationelle Selbstbestimmung – Grundlage des BDSG

Das im Grundgesetz verankerte allgemeine Persönlichkeitsrecht enthält in seiner Ausprägung als Grundrecht auf informationelle Selbstbestimmung die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und den Umgang mit den ihn betreffenden Daten zu entscheiden.
Einschränkungen dieses Rechts sind nur im überwiegenden Allgemeininteresse zulässig. Die das überwiegende Allgemeininteresse bestimmenden Voraussetzungen hat der Gesetzgeber in bereichsspezifischen und allgemeinen datenschutzrechtlichen Bestimmungen geregelt.
Bereichsspezifische Normierungen finden sich z. B. in § 29 Soldatengesetz, § 25 Wehrpflichtgesetz und §§ 106 ff. Bundesbeamtengesetz. Für Beschäftigte gilt § 3 Abs. 5 des Tarifvertrages für den öffentlichen Dienst (Bund).
Allgemeine und grundlegende Voraussetzungen beinhaltet das Bundesdatenschutzgesetz (BDSG).

3. Das Bundesdatenschutzgesetz

Das BDSG ist die allgemeine gesetzliche Grundlage für die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten.

Zweck des BDSG ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

4. Zielsetzung

Bei der Auftragserfüllung der UniBwM sind folgende datenschutzrechtliche Ziele zu berücksichtigen:
- personenbezogene Daten dürfen nur an Befugte weitergegeben werden **(Vertraulichkeit)**
- personenbezogene Daten dürfen nur unverfälscht und widerspruchsfrei verarbeitet und genutzt werden **(Integrität)**
- personenbezogene Daten müssen zeitgerecht und ordnungsgemäß verfügbar sein **(Verfügbarkeit)**
- personenbezogene Daten müssen jederzeit ihrem Ursprung zuzuordnen sein **(Authentizität)**
- es muss jederzeit überprüfbar sein, wer wann welche personenbezogenen Daten wie verarbeitet und genutzt hat **(Revisionsfähigkeit)**
- es muss jederzeit die Art der Datenverarbeitung durch eine vollständige und aktuelle Dokumentation nachvollziehbar sein **(Transparenz)**

Ferner müssen die Voraussetzungen zur Wahrung der Rechte betroffener Personen (vgl. 12.3) geschaffen werden. Beispiel: Auf Anfrage muss die betroffene Person darüber informiert werden können, welche Daten über sie gespeichert sind und woher sie stammen. Die Herkunft muss daher entsprechend vermerkt sein.

5. Die Grundsätze des Datenschutzes

Das gesamte Datenschutzrecht basiert auf folgenden Grundsätzen (dem so genannten „RETTER-Prinzip“):

5.1 Rechtmäßigkeit und Kontrolle

Der Umgang mit personenbezogenen Daten muss der rechtmäßigen Aufgabenerfüllung dienen und auf einer gesetzlichen Grundlage oder einer freiwilligen Einwilligung der oder des Betroffenen beruhen.
Die Beachtung der gesetzlichen Bestimmungen beim Umgang mit personenbezogenen Daten wird von verschiedenen Stellen aus kontrolliert. Beispiel: Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) nimmt Eingaben gegebenenfalls zum Anlass für eine Überprüfung der UniBwM.

5.2 Erforderlichkeit

Da jede Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten einen Eingriff in das Recht auf informationelle Selbstbestimmung bedeutet, dürfen die Daten nur verarbeitet werden, wenn dies zur Erfüllung der Aufgaben der UniBwM zwingend erforderlich sowie der Eingriff darüber hinaus geeignet und verhältnismäßig ist.

Bei der Datenverarbeitung muss im Interesse der/des Betroffenen die Art und Weise der Verarbeitung so gewählt werden, dass das Recht auf informationelle Selbstbestimmung der/des Betroffenen so wenig wie möglich beeinträchtigt wird und die Verarbeitungsmöglichkeiten entsprechend beschränkt werden. Bei der Verarbeitung ist nach den Grundsätzen der **Datensparsamkeit** (so wenig personenbezogene Daten wie möglich) bzw. **Datenvermeidung** (keine Erhebung personenbezogener Daten, soweit nicht erforderlich; Verarbeitung oder Nutzung in anonymisierter Form, sofern möglich) vorzugehen. Es darf nur das zur Aufgabenerfüllung erforderliche Minimum an Daten erhoben, verarbeitet und genutzt werden. Beispiel: Die Kenntnis von Augenfarbe, Blutgruppe oder Automarke o.ä. ist grundsätzlich für die Aufgabenerfüllung einer Dezernatsleiterin/eines Dezernatsleiters nicht erforderlich.

Die zulässigerweise erhobenen Daten dürfen nur solange gespeichert werden, wie sie zur Aufgabenerfüllung benötigt werden.

Zu prüfen ist daher stets,
- auf welcher gesetzlichen Grundlage der Umgang mit personenbezogenen Daten erfolgt,
- welchem konkreten Zweck der Umgang mit den personenbezogene Daten dient,
- ob der Umgang mit personenbezogenen Daten als solcher, aber auch jedes Datenfeld (z. B. Dienstgrad, Name, Vorname) erforderlich ist,
- wie konkret Datenfelder bezeichnet werden können (**keine** Felder: Bemerkungen, Sonstiges etc.),
- wie lange die personenbezogenen Daten zur Wahrnehmung der konkreten Aufgabe gespeichert werden müssen
- welche (gegebenenfalls unterschiedlichen) Löschungsfristen festgelegt werden müssen,
- wer den Zugriff auf die personenbezogenen Daten benötigt,
- wer die personenbezogene Daten innerhalb der UniBwM noch für seine Aufgabenerfüllung unter Beachtung der Zweckbestimmung benötigt,
- wie die personenbezogenen Daten gepflegt werden sollen,
- welche technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen

Daten zu ergreifen sind,
- welche Auswertungen oder Abfragen zur Aufgabenerfüllung notwendig sind.

5.3 Transparenz

Der Weg personenbezogener Daten innerhalb der UniBwM muss transparent und nachvollziehbar sein.

Aus den genannten Gründen ist zu dokumentieren:
- wie und von welcher Stelle / Person die Daten in die UniBwM gelangt sind und
- an welche Stellen (z. B. Institut, Dezernat) die Daten innerhalb der UniBwM weitergegeben worden sind sowie
- an welche andere Dienststelle (datenschutzrechtlich verantwortliche Stelle) diese übermittelt worden sind.

Nur hierüber wird die Grundlage geschaffen,

- ein Auskunftsersuchen der betroffenen Person (wie vom Gesetzgeber gefordert) überhaupt beantworten oder
- der Nachberichtspflicht entsprechen zu können, d. h. Stellen, die personenbezogene Daten erhalten haben, über die Unrichtigkeit dieser personenbezogenen Daten unterrichten zu können.

Darüber hinaus muss es möglich sein, die Art und Weise, mit der personenbezogene Daten erhoben, verarbeitet oder genutzt werden, nachvollziehen zu können. Dies setzt eine entsprechende Dokumentation voraus. Diese ist fortzuschreiben, um der Aktualitätspflicht zu genügen. Mit der Dokumentation wird an den einzelnen Stellen innerhalb der UniBwM festgelegt, wie der Umgang mit den personenbezogenen Daten erfolgen soll.

Entsprechend sind diese Dokumentationen Ausgangspunkt für Kontrollen der/des Administrativen Datenschutzbeauftragten (ADSB) der UniBwM, des Beauftragten für den Datenschutz in der Bundeswehr (BfDBw) oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI).

5.4 Technische und organisatorische Maßnahmen

Personenbezogene Daten sind innerhalb der UniBwM und bei deren Weitergabe an andere Stellen durch angemessene Maßnahmen zu sichern und zu schützen. Es sind die entsprechenden technischen und organisatorischen Maßnahmen zu treffen. Beispiele: Kennwortschutz, geschlossene Türen, Bildschirmschoner beim kurzfristigen Verlassen des Dienstzimmers aktivieren, Postversand von Personalakten nur im doppelten Umschlag mit Empfangsbekenntnis.
Daten in Akten sind ebenso zu schützen wie Daten auf anderen Speichermedien (z. B. Festplatte, Server, USB-Stick, Chip-Karte, Diskette, CD-Rom, Diktatbänder, Videobänder).

Werden personenbezogene Daten erhoben, verarbeitet oder genutzt, ist
- der Geschäftsablauf so zu gestalten, dass er den besonderen Anforderungen des Datenschutzes gerecht wird,
- Unbefugten der Zutritt zu Dienstzimmern oder Datenverarbeitungsanlagen, in denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren **(Zutrittskontrolle)**,

- zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können **(Zugangskontrolle),**
- zu gewährleisten, dass
  - auf Akten oder Schriftstücke mit personenbezogenen Daten nur Befugte zugreifen können,
  - die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können **(Zugriffskontrolle)**,
- zu gewährleisten, dass personenbezogene Daten
  - in Akten oder Schriftstücken bei ihrer Weiterleitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können sowie überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist,
  - bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist **(Weitergabekontrolle)**,
- zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind **(Eingabekontrolle)**,
- zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können **(Auftragskontrolle)**,
- zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind **(Verfügbarkeitskontrolle)**,
- zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden.

Die Art und der Umfang der zu treffenden Maßnahmen richten sich nach der Schutzbedürftigkeit der personenbezogenen Daten.

Man unterscheidet drei Schutzbereiche. Schutzbereich 1 umfasst die Funktionsträgerdaten (=Vorname, Nachname, Dienst- bzw. Amtsbezeichnung, Funktion und Tätigkeitsbereich, dienstliche Erreichbarkeit) sowie die letzten fünf Ziffern der Personenkennziffer (PK) und die Personalnummer. Diese unterliegen einem geringeren Schutz und dürfen innerhalb der UniBwM unverschlüsselt verarbeitet und übertragen werden. Die datenschutzrechtlichen Grundsätze sind selbstverständlich dennoch zu beachten. Den hohen Anforderungen des Schutzbereichs 3 unterliegen die besonderen personenbezogenen Daten, d. h. alle Daten, die zu einer Diskriminierung führen können. Alle anderen personenbezogenen Daten sind Schutzbereich 2 zugeordnet.

Bei der Erstellung und Fortschreibung des UniBwM bezogenen IT-Sicherheitskonzeptes sind die vorstehend genannten Anforderungen ebenfalls zu berücksichtigen.

Im Übrigen – also bei jeder Form der nicht-automatisierten Datenverarbeitung – sind Maßnahmen zu treffen, die der Beachtung der oben genannten Kontrollmechanismen dienen.

5.5 Einschränkung der Verfügbarkeit (Zweckbindung)

Die Daten dürfen nur für Zwecke verwendet werden, für die sie erhoben oder erfasst wurden.
Die Verarbeitung oder Nutzung personenbezogener Daten für andere Zwecke kann nur erfolgen, sofern

das ausdrücklich gesetzlich bestimmt ist oder die betroffene Person in die neue Verwendung ihrer Daten wirksam eingewilligt hat.

Ziel der Zweckbindung ist es zu verhindern, dass durch willkürliches Sammeln und Verarbeiten von personenbezogenen Daten die betroffene Person „gläsern“ wird. Deswegen ist der Grundsatz der Zweckbindung nicht nur bei der Übermittlung der Daten aus der UniBwM heraus zu beachten, sondern auch bei der Nutzung der Daten innerhalb der UniBwM.

5.6 Rechte betroffener Personen

Zum Ausgleich für den Eingriff in das Grundrecht auf informationelle Selbstbestimmung stehen jeder Person verschiedene Rechte zu (vgl. 12.3). Sie soll dadurch grundsätzlich in die Lage versetzt werden, Einfluss auf ihre Daten nehmen zu können. Beispiel: Eine Angehörige/ein Angehöriger der UniBwM ersucht um Auskunft über die zu seiner Person gespeicherten personenbezogenen Daten. Gegebenenfalls kann sie/er ihre Berichtigung verlangen.

6 Gesamtverantwortung der Leitung/einzelner Verantwortungsbereiche

6.1 Die Präsidentin/der Präsident als Leiter(in) der datenschutzrechtlich verantwortlichen Stelle

Der Präsidentin/dem Präsidenten obliegt nach den Vorgaben des Gesetzgebers die Verantwortung für die Rechtmäßigkeit beim Umgang mit personenbezogenen Daten innerhalb der UniBwM und bei ihrer Übermittlung.

Sie/Er ist beispielsweise Adressat, wenn
- die betroffene Person ihre Rechte wahrnimmt,
- eine Kontrollinstitution in der UniBwM die Beachtung datenschutzrechtlicher Bestimmungen überprüft,
- es wegen der Verletzung datenschutzrechtlicher Regelungen zu einem Bußgeldbescheid kommt.

Ihr/Ihm steht das Recht zu,
- Einzelheiten für den Umgang mit personenbezogenen Daten an der UniBwM verbindlich festzulegen,
- bei der Meldung eines Verfahrens zur automatisierten Datenverarbeitung als datenschutzrechtlich Verantwortliche(r) ausgewiesen zu werden,
- Strafantrag für den Fall eines datenschutzrechtlichen Verstoßes innerhalb der UniBwM zu stellen.

Die Präsidentin/der Präsident gewährleistet unmittelbar die Beachtung datenschutzrechtlicher Bestimmungen innerhalb der Präsidialabteilung. Sie bestellt der/dem Administrativen Datenschutzbeauftragten (ADSB), eine Ansprechpartnerin/einen Ansprechpartner für datenschutzrechtliche Angelegenheiten.

Diese/Dieser

- prüft in Zusammenarbeit mit der/dem ADSB die Rechtmäßigkeit der Erhebung personenbezogener Daten bei erstmaliger Erhebung, stellt die Unterrichtung der Betroffenen von der erstmaligen Speicherung gemäß den Rechten der betroffenen Person sicher und prüft die Rechtmäßigkeit der weiteren Verarbeitung und Nutzung der personenbezogenen Daten,

- stellt sicher, dass alle für die Meldung zum Verfahrensregister (DATAV) notwendigen Informationen der/dem ADSB zeitgerecht und umfassend zugeleitet werden,
- prüft in Verbindung mit der/dem ADSB die Notwendigkeit einer Vorabkontrolle (siehe Anlage 1),
- sichert die Bereitstellung aller Informationen zur Beantwortung eines Auskunftsersuchens.

Für die Sicherstellung des Datenschutzes im gesamten Bereich der UniBwM wird die Präsidentin/der Präsident beruhend auf der besonderen Struktur einer Universität der Bundeswehr durch folgende Stellen bzw. Organisationselemente unterstützt.

6.2 Verantwortungsbereiche, in denen der Datenschutz in Zusammenarbeit mit der/dem Administrativen Datenschutzbeauftragten (ADSB) sichergestellt wird

Im Folgenden werden alle Funktionsträger(innen) der UniBwM mit ihren Verantwortungsbereichen aufgelistet. Die restlichen unter 6.2.3 genannten Institutionen/Funktionsträger stellen die Zusammenarbeit mit der/dem ADSB sicher.

6.2.1 Die Verantwortlichkeit der Vizepräsidentinnen/Vizepräsidenten

Die Vizepräsidentinnen/Vizepräsidenten stellen die Beachtung datenschutzrechtlicher Bestimmungen in Absprache mit der/dem ADSB innerhalb ihres Verantwortungsbereichs sicher.

6.2.2 Die Verantwortlichkeit der Kanzlerin/des Kanzlers

Die Kanzlerin/der Kanzler stellt die Beachtung datenschutzrechtlicher Bestimmungen in Absprache mit der/dem ADSB innerhalb der zentralen Verwaltung sicher.

6.2.3 Verpflichtungen/Aufgaben von Institutionen/Funktionsträgern

Die Leiterinnen/Leiter der nachfolgend genannten Institutionen/Funktionsträger der Universität der Bundeswehr haben, für jeden Bereich gesondert, Ansprechpartner für datenschutzrechtliche Angelegenheiten zu benennen. Hinsichtlich ihrer Verpflichtungen und Aufgaben im Bereich des Datenschutzes unterliegen sie der Fach- und Dienstaufsicht der/des Präsidentin/Präsidenten der Universität und sind diesbezüglich weisungsgebunden.

Im Einzelnen handelt es sich um folgende Institutionen/Funktionsträger:

die Abteilungsleiter(innen)

die Leiterin/der Leiter Controlling

die Dezernatsleiter(innen)

die Dekane/die Dekaninnen

die Institutsleiter/die Institutsleiterinnen

die Professoren/die Professorinnen

die Leiterinnen/die Leiter der Zentralen Einrichtungen

die Leiterin/der Leiter Studentenbereich

der/die Zuständige für Betriebsschutz/Arbeitssicherheit

die Betriebssanitäterin/der Betriebssanitäter

Sie haben im Zusammenwirken mit dem o.g. Ansprechpartner für datenschutzrechtliche Angelegenheiten folgende Aufgaben:

- Sie prüfen in Zusammenarbeit mit der/dem ADSB die Rechtmäßigkeit der Erhebung personenbezogener Daten bei erstmaliger Erhebung, stellen die Unterrichtung der Betroffenen von der erstmaligen Speicherung gemäß den Rechten der betroffenen Person sicher und prüfen die Rechtmäßigkeit der weiteren Verarbeitung und Nutzung der personenbezogenen Daten.
- Sie stellen sicher, dass alle für die Meldung zum Verfahrensregister (DATAV) notwendigen Informationen der/dem ADSB zeitgerecht und umfassend zugeleitet werden.
- Sie prüfen in Verbindung mit der/dem ADSB die Notwendigkeit einer Vorabkontrolle (siehe Anlage 1).
- Sie sichern die Bereitstellung aller Informationen zur Beantwortung eines Auskunftsersuchens.

Soweit der angesprochene Kreis der Institutionen/Funktionsträger einen Ansprechpartner für datenschutzrechtliche Angelegenheiten des jeweiligen Bereiches namentlich benannt hat, hat dieser vertrauensvoll mit dem ADSB zusammen zu arbeiten.

6.3 Dienst- und Fachaufsicht/Sanktionen

Die Präsidentin /der Präsident ist Kontrollinstanz hinsichtlich der Einhaltung der Datenschutzbestimmungen der Universität (siehe 6.1). Sie/Er prüft unter Einbeziehung der/des ADSB bei Verstößen gegen einschlägige Rechtsvorschriften und sonstige Bestimmungen ggf. in Betracht kommende dienst-, arbeitsrechtliche oder sonstige Maßnahmen.

6.4 Verantwortungsbereiche, in denen der Datenschutz in eigener Verantwortung wahrgenommen wird

Die folgenden genannten Funktionsträger(innen) und Gremien haben innerhalb ihres Zuständigkeitsbereichs die Einhaltung des Datenschutzes und seiner geltenden gesetzlichen Bestimmungen und sonstigen Regelungen selbstverantwortlich sicherzustellen. Dies ergibt sich aus ihrem Amt oder ihrer Funktion, die entweder dem Berufsgeheimnisschutz unterliegt oder im jeweils betroffenen Tätigkeitsbereich eine erhöhte Vertraulichkeit und Unabhängigkeit erfordert.

Diese Funktionsträger(innen) unterliegen keiner datenschutzrechtlichen Kontrolle. Gleichwohl können sie sich jederzeit in grundsätzlichen datenschutzrechtlichen Angelegenheiten an die/den ADSB wenden:

- Personalrat
- Vertrauensperson der Schwerbehinderten

- Leitungsgremium
- Erweiterte Hochschulleitung
- Senat
- Verwaltungsrat
- Universitätsrat
- Konvent Wissenschaftliche Mitarbeiter
- Studentischer Konvent
- Gleichstellungsbeauftragte/Gleichstellungsbeauftragter
- Psychologisches Personal der psychologischen Beratungsstelle der Universität

6.5 Die Verantwortlichkeit der/des Administrativen Datenschutzbeauftragten (ADSB)

Das Aufgabengebiet des Datenschutzes umfasst:
- die Beratung der Leitung und Angehörigen der UniBwM in Angelegenheiten des Datenschutzes,
- das Koordinieren der Datenschutzmaßnahmen innerhalb der UniBwM,
- die Prüfung der Zulässigkeit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten in Akten und Dateien,
- die Erstellung und Fortschreibung des Datenschutzkonzeptes
- die Mitwirkung bei der Erarbeitung von Antwortschreiben auf Beschwerden, Eingaben u. ä., wenn datenschutzrechtliche Belange berührt sind,
- die Unterrichtung der Angehörigen der UniBwM in Angelegenheiten des Datenschutzes,
- das Führen der Übersicht über Verfahren zur automatisierten Verarbeitung personenbezogener Daten,
- die Erstellung von Hilfsmitteln zur Aufgabenwahrnehmung nach dem BDSG,
- die Koordinierung und Erarbeitung von Stellungnahmen auf Prüfberichte von Kontrollinstitutionen.

Das Kontrollrecht der/des ADSB erstreckt sich nicht auf die unter Ziffer 6.4 genannten Verantwortlichen.

Die/Der ADSB Datenschutzbeauftragte unterliegt der Verschwiegenheitspflicht gem. § 4f Abs. 4 BDSG. Diese umfasst insbesondere die Identität betroffener Personen.

Sollten sich innerhalb einer datenschutzrechtlich verantwortlichen Stelle Abstimmungsprobleme zwischen der fachlich zuständigen Stelle und der bzw. dem ADSB ergeben, entscheidet die Dienststellenleiterin bzw. der Dienststellenleiter in der Sache bzw. über das weitere Vorgehen. Sieht die Dienststellenleitung die Notwendigkeit für eine Bewertung durch eine vorgesetzte Dienststelle, so ist der Sachverhalt dem Fachreferat BMVg R I 1 vorzulegen.

6.6 Die Verantwortlichkeit des IT-Sicherheitsbeauftragten

Der IT-Sicherheitsbeauftragte unterstützt die Präsidentin/den Präsidentin und die/den ADSB bei deren Aufgabenwahrnehmung im Hinblick auf die automatisierte Verarbeitung personenbezogener Daten.

Bei der Erstellung und Fortschreibung des für die UniBwM geltenden IT-Sicherheitskonzeptes berücksichtigt er die technisch-organisatorischen Maßnahmen gemäß § 9 BDSG und konkretisiert die Anlage zu § 9 BDSG. Im IT-Sicherheitskonzept sind die Maßnahmen zum Schutz der personenbezogenen Daten technisch umzusetzen.

An der UniBwM unterstützt der Arbeitskreis IT-Sicherheit den IT-Sicherheitsbeauftragten (IT-SiBe) der Dienststelle.

6.7 Verantwortlichkeit der/des Verantwortlichen für den Datenschutz in der DV-Unterstützung des Personalwesens der Bundeswehr (DVUStgPersWBw)

Die Verantwortlichkeiten und Aufgaben der/des Verantwortlichen für den Datenschutz in der DVUStgPersWBw sind im Datenschutzkonzept DVUStgPersWBw UniBwM konkret beschrieben und festgelegt. Das Konzept ist im Intranet UniBwM abrufbar (vgl. Nr. 13)

7. Datenschutzrechtliche Vorgaben für spezielle Bereiche und Maßnahmen

Alle ergänzenden Regelungen sind im Intranet UniBwM abrufbar (vgl. Nr. 13)

7.1 Informationen des Rechenzentrums der UniBw München

Weiterführende Informationen zum Datenschutz im Hinblick auf das Rechenzentrum enthalten die Datenschutzerklärung des Rechenzentrums, die Hinweise zur IT-Sicherheit, die Richtlinie Mobilgeräte im Datennetz und die Datenschutzerklärung der UniBwM in Bezug auf die universitäre Homepage.

7.2 Videoüberwachung und Videoüberwachungsattrappen an der UniBwM

Jede Form der Videoüberwachung sowie auch das Anbringen von Videoüberwachungsattrappen an der UniBw München bedürfen der Genehmigung durch den ADSB. Gleiches gilt für die Änderung von bestehenden Videoüberwachungsanlagen.

8 Aus- und Fortbildung aller Angehörigen der UniBwM

Für jede/n Angehörige/n ist eine auf den Dienstposten ausgerichtete Aus- und Fortbildung im Datenschutz vorzusehen. Art und Intensität der Aus- und Fortbildung orientieren sich an der Sensitivität der personenbezogenen Daten, mit denen bei der Aufgabenwahrnehmung umgegangen wird. Hierzu sind auf Abteilungs-/Fakultätsebene und entsprechenden Stufen der übrigen Bereiche dienstpostenbezogene Festschreibungen zu treffen.

Folgende Ausrichtungen kommen in Betracht:
- Aus- und Fortbildung von Führungspersonal,
- Aus- und Fortbildung von Multiplikatoren,
- allgemeine datenschutzrechtliche Ausbildung,
- Fortbildung unter Ausrichtung auf bereichsspezifische datenschutzrechtliche Bestimmungen Soldatengesetz, Bundesbeamtengesetz, Sozialversicherungsgesetz usw.).

Die Aus- und Fortbildung kann für Führungspersonal und Multiplikatoren unter Nutzung ressortinterner oder externer Angebote erfolgen.

Die allgemeine datenschutzrechtliche Basisschulung erfolgt

- durch eine erste Orientierung bei Aufnahme der Tätigkeit in der UniBwM
- durch regelmäßig innerhalb der UniBwM von der/dem ADSB durchzuführende Veranstaltungen. Die/Der ADSB kann hierzu unterstützende ressortinterne oder geeignete externe Kräfte hinzuziehen.

Für die Information der Angehörigen der UniBwM können auch der hochschulöffentliche Bereich des Internets der UniBwM oder entsprechend geeignete technische Medien genutzt werden.

9 Der behördliche Datenschutzbeauftragte

Nach dem BDSG haben öffentliche Stellen, die personenbezogene Daten automatisiert erheben, verarbeiten oder nutzen, schriftlich einen Beauftragten für den Datenschutz zu bestellen.

Im Geschäftsbereich des BMVg wurde hierzu der Beauftragte für den Datenschutz in der Bundeswehr (BfDBw) eingerichtet und bestellt. Er nimmt zentral vom BMVg aus die zugewiesenen Aufgaben wahr.Seinen Tätigkeitsbericht legt er dem Bundesminister der Verteidigung vor.

Im Rahmen der Aufgabe, auf die Einhaltung bereichsspezifischer und allgemeiner datenschutzrechtlicher Bestimmungen hinzuwirken, steht dem BfDBw ein umfassendes Kontrollrecht zu. **Hierbei kann es auch zu unangekündigten Prüfungen kommen.**

Die Stellungnahme zum Prüfbericht erarbeitet die/der ADSB. Sie/Er ist innerhalb der UniBwM von den betroffenen Abteilungen und Bereichen zu unterstützen.
Die Stellungnahme wird von der Präsidentin/dem Präsidenten unterzeichnet. Sie ist dieser/diesem hierzu auf dem Dienstweg (innerhalb der UniBwM) vorzulegen.

Der BfDBw hat ein weitreichendes Unterrichtungsrecht. Ihm sind jeglicher Zugang zu den Räumen und jeglicher Zugriff auf personenbezogene Daten zu gewähren.

Bestehen bei der automatisierten Verarbeitung personenbezogener Daten für die betroffene Person besondere Risiken, so ist das Verfahren vor Inbetriebnahme beim BfDBw zur Vorabkontrolle anzumelden.
Besondere Risiken bestehen, wenn sensitive personenbezogene Daten verarbeitet werden oder hierbei neue technische Entwicklungen zum Einsatz kommen. Beispiel: Verarbeitung von Gesundheitsdaten oder Bemerkungen folgend aus psychologischen Untersuchungen.

Der BfDBw ist auf die Zusammenarbeit mit der/dem ADSB angewiesen.

Jede(r) Angehörige der UniBwM kann sich **unmittelbar** an den BfDBw wenden, wenn sie/er der Ansicht ist, datenschutzrechtliche Bestimmungen würden missachtet.
Der BfDBw ist zur Verschwiegenheit über die Identität dieser Person verpflichtet.

Das Kontrollrecht des BfDBw erstreckt sich nicht auf die unter Ziffer 6.4 genannten Verantwortlichen.

10 Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) wird vom Deutschen Bundestag gewählt. Ihm legt er alle zwei Jahre einen Tätigkeitsbericht vor. In diesem fasst der BfDI

die Ergebnisse seiner Beratungs- und Kontrollbesuche oder an ihn gerichtete Eingaben zusammen.

Der BfDI hat ein umfassendes Unterrichtungsrecht. Ihm sind jeglicher Zugang zu den Räumen und jeglicher Zugriff auf personenbezogene Daten zu gewähren.

Prüfberichte und förmliche Beanstandungen leitet der BfDI dem BMVg zu.

Zur Fertigung der Stellungnahme auf den Prüfbericht arbeitet die/der ADSB dem BMVg unmittelbar zu. Die/der ADSB ist bei Kontrollbesuchen des BfDI innerhalb der UniBwM von den betroffenen Abteilungen zu unterstützen.

11 Verfahrens- und Prüfabläufe

11.1 Behandlung von zentral vorgegebenen Vorhaben

Bei derartigen Vorhaben (z. B. SAP) ist davon auszugehen, dass die anordnende Stelle die datenschutzrechtlichen notwendigen Prüfschritte bereits durchgeführt hat. Die/der ADSB ist über die Nutzung solcher Vorhaben innerhalb der UniBwM durch die/den Vorhabensverantwortlichen in Kenntnis zu setzen.

11.2 Verfahrens- und Prüfabläufe innerhalb der UniBwM

Um die Einhaltung bereichsspezifischer und allgemeiner datenschutzrechtlicher Bestimmungen bereits bei der Planung sicherzustellen, sind automatisierte Verarbeitungen (z. B. Datenbank mit Betriebsdaten oder Stellenbesetzungsliste usw.), die auf den Umgang mit personenbezogenen Daten zielen, frühzeitig und umfassend mit der Ansprechpartnerin/dem Ansprechpartner für datenschutzrechtliche Angelegenheiten der Organisationseinheit und der/dem ADSB zu erörtern. Der IT-SiBe und der Beirat des Leitungsgremiums IKIS sind bei personenbezogenen Daten, die den Schutzbereichen 2 und 3 unterliegen, einzubinden (siehe 5.4).

Wegen der zu wahrenden Transparenz sind hierbei die tragenden, datenschutzrechtlich relevanten Erwägungen zu dokumentieren.

Automatisierte Verarbeitungen von personenbezogenen Daten sowie alle Änderungen an deren Struktur sind vor Nutzungsbeginn/-änderung der/dem ADSB zur Freigabe vorzulegen, um die Aufnahme in das Melderegister für automatisierte Verarbeitungen (DATAV) sicherzustellen.

Vor der Meldung von Verfahren zur automatisierten Verarbeitung (AV) in das DATAV-Register ist zu prüfen, ob das Vorhaben vorabkontrollpflichtig ist (siehe Anlage 1).

Zu berücksichtigen sind vor der Meldung in DATAV eventuelle beteiligungsrechtliche Tatbestände. In Zweifelsfällen sind gegebenenfalls die Kanzlerin/der Kanzler und je nach Organisationseinheit die Abteilungsleiter(innen), Dekane und alle weiteren mit Leitungsfunktionen ausgestatteten Personen einzubeziehen.

Datenschutzrechtliche Fragestellungen sind zunächst innerhalb der UniBwM unter Einbindung der/des ADSB zu klären. Ist auf diesem Wege eine Klärung nicht zu erreichen, ist über den Sachverhalt nebst Bewertung, bisher veranlasster Maßnahmen sowie eines Vorschlages dem BMVg zu berichten.

BMVg entscheidet über eine Anrufung des BfDBw oder des BfDI.

Im Fall der Eingabe betroffener Personen an den BfDBw oder den BfDI besteht keine Bindung an den Dienstweg – diese Kontrollinstitutionen können unmittelbar angeschrieben werden.

12 Weitere Vorgaben des BDSG zum Umgang mit personenbezogenen Daten

Alle in der UniBwM einzuleitenden und durchzuführenden Maßnahmen sind auf die oben unter 4. dargestellten Ziele und unter 5. genannten Prinzipien auszurichten. Weiterhin sind die folgenden Grundsätze zu beachten:

12.1 Datenpflege

Personenbezogene Daten unterliegen der Veränderung und sind daher je nach Art und Zweck ständig oder anlassbezogen auf ihre Richtigkeit zu überprüfen und gegebenenfalls zu pflegen,
d. h. zu berichtigen.

12.2 Datensicherung

Personenbezogene Daten müssen zur Aufgabenerfüllung jederzeit kurzfristig verfügbar sein. Daher sind die zur Datensicherung notwendigen Maßnahmen nach dem vom Rechenzentrum festgelegten Verfahren durchzuführen.

12.3 Rechte der betroffenen Person

Eine betroffene Person hat – abgeleitet aus dem Umgang mit ihren personenbezogenen Daten – nachstehende Rechte:

- **Recht auf Unterrichtung** über die Identität der UniBwM als datenschutzrechtlich verantwortliche Stelle, die Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung sowie die Kategorien von Empfängern der Daten,
- **Recht auf Benachrichtigung**, wenn die personenbezogenen Daten ausnahmsweise nicht unmittelbar bei der betroffenen Person erhoben worden sind,
- **Recht auf Auskunft** über die zu ihrer Person gespeicherten Daten, über deren Herkunft, über die Empfänger der personenbezogenen Daten innerhalb und außerhalb der UniBwM sowie über den Zweck ihrer Speicherung,
- **Recht auf Berichtigung**, wenn die Daten unrichtig gespeichert sind,
- **Recht auf Nachberichtigung**, wenn unrichtige Daten zwischenzeitlich an andere Stellen weitergegeben oder übermittelt worden sind,
- **Recht auf Löschung**, wenn die Speicherung unzulässig war oder die Kenntnisnahme der personenbezogenen Daten für die Aufgabenerfüllung der UniBwM nicht mehr erforderlich ist,
- **Recht auf Sperrung**, wenn Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen der betroffenen Person beeinträchtigt würden, sie die Korrektheit bestreitet und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt,
- **Recht auf Folgenbeseitigung,**

- **Recht auf Widerspruch** gegen die automatisierte Verarbeitung ihrer personenbezogenen Daten,
- **Recht auf Schadensersatz,**
- **Recht, sich** an den BfDBw oder den BfDI **zu wenden**, wenn die betroffene Person der Ansicht ist, bei der Verarbeitung ihrer personenbezogenen Daten in ihren Rechten verletzt zu sein,
- **Recht auf Beantragung** der Einleitung eines Bußgeldverfahrens **und**
- **Recht auf Stellung eines Strafantrags.**

Das Handeln in der UniBwM ist darauf auszurichten, diese Rechte zu gewährleisten wird.

Eine Erklärung zum Verzicht auf diese Rechte ist unzulässig und daher ggf. unwirksam.

12.4 Kontrollen

Für Kontrollen der/des ADSB, des BfDBw oder des BfDI sind
- die Dokumente / Grundlagen, die die maßgebenden datenschutzrechtlichen Erwägungen beinhalten, in den Abteilungen/Dezernaten/Fakultäten/Instituten/Zentralen Einrichtungen und sonstigen Organisationseinheiten griffbereit und aktualisiert vorzuhalten. Beispiel: Dokumentation der Schlüsselordnung, Zugangsberechtigung zu bestimmten Aktenschränken, in denen Listen mit personenbezogenen Daten aufbewahrt werden. (Siehe zudem die Dokumentationspflichten unter 5.3 Transparenz).
- technische Voraussetzungen zu schaffen, die im Fall automatisierter Datenverarbeitung eine Auswertung der Protokolldaten mit Genehmigung der Präsidentin/des Präsidenten, des Personalrats und gegebenenfalls weiterer (übergeordneter) Stellen ermöglichen. Der BfDI oder der BfDBw können jederzeit Zugriff erhalten.

Im Bereich der unter 6.4 genannten Stellen darf aufgrund der Interessenwahrung **keine** Kontrolle durchgeführt werden.

Zugang zu DATAV erhalten BfDBw und BfDI über die/den ADSB.

13 Hinweise zu weiterführenden Informationen

Die Grundlagen und Bezugsdokumente sowie weitere Informationen, Hinweise, Merkblätter und Arbeitshilfen werden allen Angehörigen der UniBw München, im hochschulöffentlichen Bereich des Intranets (zu finden auf der Homepage unter: Downloads → Bereich der Zentralen Verwaltung → Formulare und Informationen der Zentralen Verwaltung → Datenschutz) zur Verfügung gestellt.

14 Anlagen

1. Glossar
2. Abkürzungsverzeichnis

15 Inkraftsetzung

Hiermit setze ich das Datenschutzkonzept der Universität der Bundeswehr München in Kraft.
Es ersetzt das Datenschutzkonzept der Universität der Bundeswehr München vom 15.09.2010.

Neubiberg, den 01. Juni 2016 _____

Siegfried Rapp (Kanzler)

Anlage 1 - Glossar

Anonymisieren
bedeutet die Veränderung personenbezogener Daten, so dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht oder nur mit unverhältnismäßig großem Aufwand einer bestimmbaren oder bestimmten Person zugeordnet werden können.

Automatisiertes Abrufverfahren
ist eine Möglichkeit der Übermittlung personenbezogener Daten. Durch den Abruf können Daten übermittelt werden. Bei den entsprechenden Verfahren handelt es sich um Onlineverfahren der verantwortlichen Stellen mit Dritten (z. B. SAP).

Automatisierte Verarbeitung (AV)
Sie liegt vor, wenn die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen erfolgt. Sie löst für die verantwortliche Stelle die grundsätzliche Meldepflicht zum „Melderegister für automatisierte Verarbeitungen – DATAV“ aus und zwingt diese zu technischen und organisatorischen Maßnahmen gem. § 9 BDSG. Darüber hinaus ist die Notwendigkeit einer Vorabkontrolle gemäß § 4d Abs. 5 BDSG zu prüfen.

Bereichsspezifische Regelungen
sind Rechtsvorschriften des Bundes, in denen zu bestimmten Aufgabengebieten der Umgang mit personenbezogenen Daten speziell geregelt ist sowie die Befugnisse zur Erfüllung dieser Aufgaben. Sie sind den allgemeinen Regelungen des Bundesdatenschutzgesetzes gegenüber vorrangig anzuwenden.

Betroffene(r)/betroffene Person
Person, deren personenbezogene Daten erhoben, verarbeitet oder genutzt werden

Bestimmte Person
Es wird von einer bestimmten Person gesprochen, wenn ein unmittelbarer Bezug zur Person vorhanden ist.

Bestimmbare Person
Es wird von einer bestimmbaren Person gesprochen, wenn sich ein Zusammenhang zu einer Person ohne besonderen Aufwand herstellen lässt. Eine Matrikelnummer beispielsweise macht eine Person bestimmbar, wenn auch nur für einen eingeschränkten Benutzerkreis.

DATAV
ist das Melderegister für automatisierte Datenverarbeitungen (abgeleitet vom früheren Begriff Dateienerfassungs- und Auswerteverfahren zur Ausführung des BDSG“).

Datenverarbeitung im Auftrag
ist das Betrauen einer öffentlichen oder nicht-öffentlichen Stelle außerhalb der Dienststelle (der datenschutzrechtlich verantwortlichen Stelle) mit einer Datenerhebung, Verarbeitung oder Nutzung personenbezogener Daten.

Datenverarbeitungsanlage
ist eine Anlage, die über Programme verfügt, welche Inhalte in Abhängigkeit von ihrem personenbezogenen Informationsgehalt behandeln können, also Arbeitsschritte wie das Lesen und Vergleichen von Daten programmgesteuert ablaufen lassen.

Dritte(r)
ist jede Person oder Stelle außerhalb der Dienststelle.

Empfänger
ist jede Person oder Stelle, die Daten erhält.

Erheben
ist das Beschaffen von Daten über die/den Betroffene(n). Es gilt der Grundsatz der Direkterhebung, d. h. dass personenbezogene Daten grundsätzlich vorrangig bei der betroffenen Person selbst zu erheben sind und sie über den Grund der Erhebung unterrichtet werden muss.

Löschen
bedeutet das Unkenntlichmachen gespeicherter personenbezogener Daten.

Nicht automatisierte Datei
ist jede nicht automatisierte Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten, mindestens zwei personenbezogenen Merkmalen zugänglich ist und ausgewertet werden kann. Beispiele sind Sammlungen ausgefüllter Formulare.

Nutzen
ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt. Der Tatbestand ist auch erfüllt bei Weitergabe innerhalb der Dienststelle, da dabei keine Übermittlung an Dritte vorliegt.

Personenbezogene Daten
sind einzelne Angaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffene(r)). Bestimmbar ist eine Person, wenn mit den Mitteln und Möglichkeiten, die der speichernden Stelle zur Verfügung stehen, ohne unverhältnismäßigen Aufwand aus Angaben ein Bezug zu einer bestimmten Person hergestellt werden kann (z. B. über Personenkennziffer). Die Bestimmbarkeit kann sich auch aus der Kombination verschiedener Daten, die in Bezug auf eine Person gesammelt sind, ergeben.

Unterfälle:

Allgemeine personenbezogene Daten
sind personenbezogene Daten, die nicht den besonderen Arten personenbezogener Daten im Sinne des § 3 Abs. 9 BDSG zuzuordnen sind.

Besonderen Arten personenbezogener Daten
sind Angaben gemäß § 3 Abs. 9 BDSG über die rassische und ethnische Herkunft, politische Meinung, religiöse oder philosophische Überzeugung, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

Sonderfall Personalaktendaten
Hierbei kann es sich sowohl um allgemeine personenbezogene Daten als auch um besondere Arten personenbezogener Daten handeln. Um eine sachgerechte Bewertung und Schutzbereichszuordnung treffen zu können, muss daher jedes Personalaktendatum hinsichtlich seiner Art und Schutzbedürftigkeit gesondert beurteilt werden.

Pseudonymisieren
bedeutet das Ersetzen des Namens und anderer Identifikationsmerkmale einer Person durch ein Kennzeichen, wodurch die Bestimmung der/s Betroffenen ausgeschlossen oder wesentlich erschwert wird. Der wesentliche Unterschied zum Anonymisieren besteht darin, dass es eine Zuordnungsregelung gibt, dessen Kenntnis die Zuordnung des Kennzeichens (Pseudonyms) zu einer bestimmten Person ermöglicht. Demzufolge bleiben pseudonymisierte Daten für die Stelle, die die Zuordnungsregel kennt, weiterhin personenbezogene Daten.

Schutzbereich
bedeutet die Bestimmung der Schutzbedürftigkeit personenbezogener Daten, woraus sich, abhängig von der Einstufung 1, 2 oder 3 entsprechende technische und organisatorische Schutzmaßnahmen ergeben.

Speichern
bedeutet das Erfassen, Aufnehmen oder Aufbewahren von personenbezogenen Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung.

Sperren
ist das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken

Umgang mit personenbezogenen Daten
umfasst die Phasen der Erhebung, Verarbeitung (Speichern, Verändern, Übermitteln, Sperren und Löschen) und Nutzung.

Übermitteln
ist die Bekanntgabe gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten. Die Übermittlung kann entweder durch Weiterleitung erfolgen oder dadurch, dass der Dritte die Daten einsieht oder abruft.

Verantwortliche Stelle
ist jede Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Im Regelfall ist darunter eine Dienststelle oder Einheit zu verstehen.

Verarbeiten
ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten.

Verändern
ist das inhaltliche Umgestalten gespeicherter personenbezogener Daten.

Vorabkontrolle
ist die Prüfung von automatisierten Verarbeitungen durch den Bundesbeauftragten für den Datenschutz in der Bundeswehr (BfDBw) vor Beginn des Verarbeitungsprozesses, soweit die automatisierte Verarbeitung besondere Risiken für die Freiheit und Rechte der Betroffenen birgt. Das ist insbesondere dann der Fall, wenn besondere personenbezogene Daten gemäß § 3 Abs. 9 BDSG verarbeitet werden (wie z. B. medizinische Daten, Daten über Religionszugehörigkeit) oder wenn die verarbeiteten Daten die Beurteilung von Fähigkeiten, Leistung und Verhalten der betroffenen Personen ermöglichen (z. B. Sportleitungsnachweise, Arbeitszeiterfassung, LSF).

Weitergabe
ist die Datenübermittlung innerhalb einer Dienststelle.

Anlage 2 – Abkürzungsverzeichnis

Abs.	Absatz
ADSB	Administrativer Datenschutzbeauftragter
AK IT-Sicherheit	Arbeitskreis IT-Sicherheit
AV	Automatisierte Verarbeitung
BDSG	Bundesdatenschutzgesetz
BfDBw	Beauftragter für den Datenschutz in der Bundeswehr
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BMVg	Bundesministerium der Verteidigung
bzw.	Beziehungsweise
CASC	Campus Advanced Studies Center
DATAV	Melderegister für automatisierte Verarbeitung
d. h.	das heisst
etc.	et cetera
DV	Datenverarbeitung
IKIS	Informations- und Kommunikationsinfrastruktur (Beirat des Leitungsgremiums)
IT	Informationstechnologie
IT-SiBe	IT-Sicherheitsbeauftragter
SAP	ist eine Software für Personalwesen
TVöD	Tarifvertrag für den öffentlichen Dienst
u. ä.	und ähnliches (Ähnliches)
UniBwM	Universität der Bundeswehr München
usw.	und so weiter
z. B.	zum Beispiel