

## Geschäftsanweisung

**Betreff:**

### **Datenschutz**

A6 - II 1501 Datenschutz allgemein

<b>Geschäftsanweisung Nr.</b>  <b>01/2014</b>  vom 06.01.2014
Änderungen:
Verteiler: Alle Mitarbeiter Jobcenter  Aktenzeichen: II 1501

Die Geschäftsanweisung 1/2014 zur Regelung des Sozialdatenschutzes im Jobcenter Bad Doberan tritt zum 01.01.2014 in Kraft. Alle bisherigen Regeln werden damit aufgehoben.

### Inhaltsübersicht:

01. Ziel des Datenschutzes
02. Verantwortlichkeiten
03. Wesentliche Grundlagen des Datenschutzes
04. Grundsätze des Datenschutzes und Übermittlung personenbezogener Daten
05. Aufbewahrung von Unterlagen
06. Transport von Unterlagen
07. Vernichtung von Daten/Entsorgung von Schriftgut
08. IT-Sicherheit
09. E-Mail und FAX-Schriftverkehr
10. Schulungen / Belehrungen / Dienstbesprechungen
11. Kontrolle der Einhaltung des Datenschutzes
12. Inkrafttreten

### Anlagen

Anlage 1 Beauftragte für Datenschutz (wurde entfernt)

Anlage 2 Grundsätze zur zwingenden Beteiligung des/der Datenschutzbeauftragten und das Verfahren zur Beteiligung

Anlage 3 Übersicht über die Übermittlungstatbestände des SGB

Anlage 4 Unterstützende Links

## 1. Ziel des Datenschutzes

Grundsätzlich hat jede/r Einzelne das Recht, zu bestimmen, wem sie/er ihre/seine persönlichen Daten preisgibt. Jede/r ist „Herr ihrer/seiner Daten“. Gleichzeitig hat jede/r Einzelne grundsätzlich einen Anspruch darauf, zu wissen, welche Daten über sie/ihn bei welcher Stelle gespeichert sind oder auf sonstige Weise verarbeitet werden.

Ziel aller Maßnahmen zum Datenschutz und zur Geheimhaltung ist es somit, personenbezogene Daten vor Missbrauch, unbefugtem Zugriff und gegen Fehler bei der Datenverarbeitung zu schützen.

Alle Mitarbeiter/innen des Jobcenters haben beim Umgang mit personenbezogenen Daten die zum Schutz des Persönlichkeitsbereichs und der Privatsphäre des Bürgers erlassenen datenschutzrechtlichen Bestimmungen, insbesondere des Sozialgesetzbuches, des Bundesdatenschutzgesetzes und des Informationsfreiheitsgesetzes sowie diesbezügliche Weisungen zu beachten.

Allen Mitarbeitern/innen des Jobcenters ist es untersagt, geschützte personenbezogene Daten unbefugt zu einem anderen als dem zur jeweiligen Aufgabenerfüllung gehörenden Zweck zu verarbeiten, bekannt zu machen oder auf eine andere Art zu nutzen. Die bestehende Verpflichtung zur Verschwiegenheit besteht auch nach Beendigung der Tätigkeit fort. Mitarbeiter/innen, die gegen das Datengeheimnis verstoßen, verletzen damit ihre dienstrechtlichen bzw. arbeitsvertraglichen Pflichten.

Der Datenschutz ist auch bei eingesetzten Kräften von außerhalb (Dienstleistungsunternehmen, insbesondere Reinigungspersonal) sicherzustellen.

## 2. Verantwortlichkeiten

Die Gesamtverantwortung für die ordnungsgemäße Durchführung der nach dem Bundesdatenschutzgesetz (BDSG) und dem SGB X notwendigen Datenschutzmaßnahmen im Jobcenter Bad Doberan obliegt dem Geschäftsführer.

Hierbei wird er von der/dem Datenschutzbeauftragten prüfend und beratend unterstützt. Die/der schriftlich bestellte Beauftragte für den Datenschutz fungiert als Ansprechpartner/in für Kunden und Mitarbeiter in allen Fragen des Datenschutzes und wirkt auf die Einhaltung der gesetzlichen Regelungen und Vorschriften des Datenschutzes durch Beratung und Kontrolle hin. Dabei hat der/die Beauftragte für Datenschutz insbesondere die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden, zu überwachen. Darüber hinaus hat sie/er die mit der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften und Erfordernissen des Datenschutzes vertraut zu machen. Die/der Beauftragte für Datenschutz ist auch bei der datenschutzkonformen Gestaltung von Geschäftsprozessen, Vordrucken und Verträgen mit einzubeziehen.

Die/der Datenschutzbeauftragte ist dem Geschäftsführer unmittelbar unterstellt und fachlich weisungsfrei.

Die/der Beauftragte für den Datenschutz wird schriftlich bestellt und ist intern sowie auch extern durch geeignete Maßnahmen bekannt zu machen. Zur Information der Kunden sind hierbei Name und Organisationseinheit der/des Datenschutzbeauftragten bzw. des Stellvertreters/der Stellvertreterin sowie Kontaktmöglichkeiten zu veröffentlichen.

Zur Person der/des Beauftragten für Datenschutz bzw. seines Stellvertreters siehe **Anlage 1**. Grundsätze zur zwingenden Beteiligung der/des Beauftragten für Datenschutz und das in dem Zusammenhang durchzuführende Verfahren sind in der **Anlage 2** geregelt.

### 3. Wesentliche Grundlagen des Datenschutzes

Die für die Aufgabenerledigung notwendigen Informationen und Vorgaben zur Durchführung des Datenschutzes sind umfassend in den „Datenschutzbestimmungen für die Bundesagentur für Arbeit“ (DatBest) aufgeführt. Darin enthalten sind die wichtigsten Anwendungsbereiche des Datenschutzes in rechtlicher und praktischer Hinsicht, zur Erhebung, Verarbeitung und Nutzung von Sozialdaten sowie zur Übermittlung von Sozialdaten an Dritte. Siehe hierzu folgenden Link:

<http://www.baintern.de/bund/generator/goto?id=352574>  
>>> Datenschutzbestimmungen für die Bundesagentur für Arbeit

### 4. Grundsätze des Datenschutzes und Übermittlung personenbezogener Daten

Die Grundsätze des Datenschutzes sind von allen Mitarbeiterinnen und Mitarbeitern des Jobcenters im täglichen Umgang mit personenbezogenen Daten zu beachten.

Dies sind insbesondere:

- Verbot mit Erlaubnisvorbehalt
- Datenvermeidung und -sparsamkeit
- Erforderlichkeitsgrundsatz
- Transparenzgebot
- Zweckbindungsprinzip
- Verhältnismäßigkeitsgrundsatz
- Ersterhebungsgrundsatz

**Die Weitergabe personenbezogener Daten an Dritte (Übermittlung)** ist grundsätzlich restriktiv zu handhaben. Es gilt das Verbotsprinzip mit Erlaubnisvorbehalt, d. h. dass alle Übermittlungen verboten sind, die nicht ausdrücklich erlaubt sind.

Zur Übermittlung muss die Einwilligung der betroffenen Person vorliegen oder eine gesetzliche Übermittlungsbefugnis nach den §§ 68 bis 77 SGB X gegeben sein. Einen Überblick über die gesetzlichen Übermittlungstatbestände nach dem SGB X gibt die **Anlage 3**. Darin wird gleichzeitig der zu übermittelnde Datenumfang bei Anwendung der verschiedenen Rechtsvorschriften aufgezeigt.

Grundsätzlich sind sämtliche Auskunftersuchen nur in Schriftform (Brief oder Fax, nicht jedoch per E-Mail) zu akzeptieren und ebenso zu beantworten.

Auf die telefonische Weitergabe schutzwürdiger Daten an Personen und Stellen außerhalb des Jobcenters kann im Interesse wirtschaftlichen Verwaltungshandelns jedoch grundsätzlich nicht verzichtet werden. Der Auskunftserteilende muss sich dabei stets vergewissern, ob der Anrufer selbst zum Empfang der Auskunft berechtigt ist (Rückruf, gezielte Fragestellung etc.). Bei Zweifeln an der Identität ist die Übermittlung zunächst zu verweigern und dem Anrufer anheim zu stellen, persönlich vorzusprechen oder sein Anliegen schriftlich vorzubringen.

Über die Erforderlichkeit und Zulässigkeit der Übermittlung von Sozialdaten an Dritte, die über die Tagesroutine (insbesondere häufig vorkommende, gleichartige Fallgestaltungen) hinausgehen, entscheiden mindestens die Teamleiter.

Übermittlungsersuchen nach **§ 68 SGB X** (Übermittlung von Sozialdaten für Aufgaben der Polizeibehörden, der Staatsanwaltschaften und Gerichte, der Behörden der Gefahrenabwehr oder zur Durchsetzung öffentlich-rechtlicher Ansprüche), **§ 72 SGB X** (Übermittlung für den Schutz der inneren und äußeren Sicherheit) und **§ 73 SGB X** (Übermittlung für die Durchführung eines Strafverfahrens) sind dem Geschäftsführer bzw. seinem allgemeinen Stellvertreter zur weiteren Entscheidung vorzulegen.

Der Geschäftsführer, sein allgemeiner Stellvertreter bzw. ein besonders bevollmächtigter Bediensteter entscheidet über Amtshilfeersuchen der Strafverfolgungsbehörden bezüglich der Übermittlung eines geplanten Vorsprachetermins eines Kunden/einer Kundin unter Prüfung folgender Voraussetzungen:

- Anfrage einer Polizeibehörde, einer Staatsanwaltschaft oder eines Gerichts,
- Vorliegen einer Anfrage in Schriftform (Brief oder Fax, nicht jedoch per E-Mail),
- Begründung der ersuchenden Stelle, weshalb der Aufenthalt des Kunden nicht auf andere Weise festgestellt werden konnte,
- das Ersuchen darf nicht länger als sechs Monate zurückliegen

und folgenden Aspekten:

- grundsätzlich soll kein Vorsprachetermin lediglich zum Zweck der Strafverfolgung vereinbart werden,
- zum Schutz von Mitarbeitern und Kunden soll die Strafverfolgungsbehörde gebeten werden, eine eventuelle Festnahme nach Möglichkeit außerhalb des Dienstgebäudes durchzuführen (siehe auch HEGA 06/09 -11).

In Fragen des Zugriffsschutzes für gespeicherte Sozialdaten von Mitarbeiterinnen und Mitarbeitern gemäß § 35 Abs. 1 Satz 3 SGB I ist der/die Leiter/in Personal/ Finanzen beauftragt.

## **5. Aufbewahrung von Unterlagen**

Sämtliche Unterlagen mit personenbezogenen Daten sind am Arbeitsplatz nur so lange aufzubewahren, wie es für die Erledigung der fachlichen Aufgaben unbedingt erforderlich ist. Sie dürfen nur den dienstlich damit befassten Mitarbeiterinnen und Mitarbeitern zugänglich gemacht werden. Ansonsten sind sie unter Verschluss zu halten, d. h. die Unterlagen sind gesichert aufzubewahren.

Unterlagen mit personenbezogenen Daten sind in mit Sicherheitsschlössern verschließbaren Räumen unter Verschluss zu halten. Werden Unterlagen mit personenbezogenen Daten in nicht mit Sicherheitsschlössern verschließbaren Räumen aufbewahrt, so sind sie in mit Sicherheitsschlössern ausgestatteten Behältnissen/Schränken unter Verschluss zu halten. Räume, in denen schutzwürdige Daten unverschlossen aufbewahrt werden, dürfen nicht ohne Aufsicht bleiben.

Bei vorübergehendem Verlassen der Diensträume während der Dienststunden und nach Dienstschluss sind die Zimmertüren zu verschließen.

Es ist sicherzustellen, dass mit der Sache nicht befassten Personen, insbesondere dem Reinigungspersonal, keine Einsicht in Unterlagen möglich ist. Insoweit sollen die Unterlagen mit den schutzwürdigen Daten nach Dienstschluss der Mitarbeiter grundsätzlich in den Schränken verschlossen sein.

Mitarbeiter mit einem mobilen Arbeitsplatz (MAP) haben ebenso dafür Sorge zu tragen, dass unbefugte Personen keine Kenntnis von schutzwürdigen Daten erhalten können. Der MAP ist stets so aufzubewahren, dass er vor unbefugtem Zugriff sicher ist.

Es ist nicht zulässig, Akten und sonstige Schriftstücke mit personenbezogenen Daten mit nach Hause zu nehmen. Ausnahmen hiervon sind nur nach vorheriger Zustimmung durch die zuständigen Teamleiter möglich.

Beim Drucken datenschutzrelevanten Schriftgutes ist sicherzustellen, dass keine Einsichtnahme unbefugter Personen erfolgen kann.

## **6. Transport von Unterlagen**

Beim Transport von Unterlagen mit personenbezogenen Daten durch Boten oder andere Beschäftigte ist darauf zu achten, dass eine unbefugte Einsicht oder Mitnahme sowie der Verlust von Teilen oder des gesamten Transportgutes ausgeschlossen sind. Die Transportwagen/-behälter dürfen daher auf keinen Fall unbeaufsichtigt gelassen werden. Für den Transport von besonders vertraulichen Unterlagen (z.B. Personalangelegenheiten, Beurteilungen usw.) sind Verschlussmappen zu verwenden.

## **7. Vernichtung von Daten/Entsorgung von Schriftgut**

Personenbezogene Daten, die zur Vernichtung freigegeben sind, müssen sicher gelöscht bzw. vernichtet werden.

Datenschutzwürdige Unterlagen auf Papier müssen speziell entsorgt werden und grundsätzlich in die speziell hierfür zur Verfügung stehenden Datenschutzcontainer gegeben werden. Diese werden dann weiter von einem mit der datenschutzgerechten Vernichtung beauftragten Unternehmen gemäß Bundesdatenschutzgesetz vernichtet. Bei größeren Mengen oder Sonderaktionen (z.B. Aktenaussonderung) hat eine gesonderte Abholung und Zuführung zur gesicherten Vernichtung durch das beauftragte Unternehmen zu erfolgen.

## **8. IT-Sicherheit**

Durch die Führungskräfte ist abzusichern, dass jede Mitarbeiterin/jeder Mitarbeiter des Jobcenters über die Rollenkonzepte nur die Berechtigungen für IT-Verfahren erhält, die zwingend für die Arbeitserledigung erforderlich sind. Die Berechtigungen sind insoweit in regelmäßigen Abständen durch die Teamleiter bzw. die zuständige Führungskraft zu prüfen. Der Zugang zum Computernetzwerk und den einzelnen Anwendungsprogrammen ist durch Passwörter geschützt. Diese Passwörter sind an die Person des jeweiligen Mitarbeiters / der Mitarbeiterin gebunden. Es ist untersagt, Passwörter an Dritte weiterzugeben oder auf andere Weise ihren unbefugten Gebrauch zu ermöglichen. Bekannt gewordene Passwörter sind umgehend zu ändern.

Bei vorübergehendem Verlassen des Arbeitsplatzes ist der Computer durch den jeweiligen Mitarbeiter/ die jeweilige Mitarbeiterin zu sperren.

## **9. E-Mail und FAX-Schriftverkehr**

In E-Mails und PC-Fax-Mitteilungen im BA-internen Netz sollen vertrauliche personenbezogene Daten nur so sparsam wie möglich enthalten sein. Klarnamen dürfen in Betreffzeilen generell nicht enthalten sein – Abkürzungen und Anonymisierungen sind jedoch zulässig.

Beim Versand sensibler Daten per Telefax ist besondere Sorgfalt geboten: es muss sichergestellt sein, dass die gewählte Anschlussnummer gültig ist, dass die Sendung nur dem gewünschten Empfänger zugeht und dass der Telefax-Einsatz aufgrund besonderer Eilbedürftigkeit erforderlich ist.

Datenschutzrechtliche Regelungen gelten auch für die Aufbewahrung von E-Mails oder Fax-Mitteilungen, die personenbezogene Daten enthalten. Diese dürfen nur so lange aufbewahrt werden, wie dies tatsächlich für die Aufgabenerledigung erforderlich ist. Nach Ablauf entsprechender Fristen sind diese zu löschen.

## **10. Schulungen / Belehrungen / Dienstbesprechungen**

Diese Geschäftsanweisung sowie die eingangs genannten Datenschutzbestimmungen der Bundesagentur für Arbeit sind mindestens einmal jährlich zum Gegenstand von Dienstbesprechungen in den einzelnen Organisationseinheiten zu machen. Darüber hinaus ist die auf die Tagesarbeit der Mitarbeiter/innen ausgerichtete Behandlung des Themas „Sozialdatenschutz“ kontinuierlich, und nicht nur anlassbezogen, mit jeweiligen Schwerpunkten in den einzelnen Organisationseinheiten sicherzustellen.

Die Durchführung ist in den entsprechenden Protokollen ausreichend zu dokumentieren. Verantwortlich für die Durchführung und Dokumentation sind die Teamleiter bzw. die zuständigen Führungskräfte.

Bei der Einstellung und Einarbeitung neuer Mitarbeiter/innen ist der Sozialdatenschutz regelmäßig mit einzubeziehen. Insoweit hat vor Aufnahme der Beschäftigung bereits eine entsprechende Belehrung der jeweiligen Mitarbeiter zu erfolgen. Im Jobcenter eingesetzte Kräfte von außerhalb, insbesondere die Reinigungskräfte, sind nachweislich zum Datenschutz zu belehren.

## **11. Kontrolle der Einhaltung des Datenschutzes**

Die Einhaltung der datenschutzrechtlichen Vorschriften und Weisungen sind kontinuierlich und in regelmäßigen Abständen in den einzelnen Organisationseinheiten im Rahmen der Fachaufsicht durch die Führungskräfte zu kontrollieren. Die Kontrollergebnisse sind schriftlich zu dokumentieren.

Mindestens einmal jährlich sind die Ergebnisse unter Beteiligung der/des Beauftragten für Datenschutz schriftlich zu bewerten. Im Nachgang sind unter Beteiligung der/des Beauftragten für Datenschutz geeignete Maßnahmen zur Reduzierung der festgestellten Mängel einzuleiten und systematisch nachzuhalten.

Die/der Datenschutzbeauftragte informiert den Geschäftsführer über die Ergebnisse der durchgeführten Kontrollen und die weiteren Festlegungen.

## **12. Inkrafttreten**

Diese Geschäftsanweisung tritt zum 01.01.2014 in Kraft.

Alle bisher ergangenen Weisungen und Verfügungen zum Datenschutz werden damit aufgehoben.

Der Personalrat wurde informiert.

## **Grundsätze zur zwingenden Beteiligung des/der Datenschutzbeauftragten und das Verfahren zur Beteiligung**

Jede Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt, muss vor jeder Entscheidung, die sich auf die Verarbeitung personenbezogener Sozial- oder Personaldaten auswirkt, und zwar nicht nur bei automatisierten Vorhaben, die/den Datenschutzbeauftragte/n informieren und konsultieren. Dies gilt für sämtliche Formen und Phasen der Verwendung personenbezogener Daten. Sie ist verpflichtet, die/den Datenschutzbeauftragte/n in die Lage zu versetzen, ihre/seine Auffassung rechtzeitig und eindeutig zu dem jeweiligen Vorhaben zur Geltung zu bringen. Auch wenn eine nachträgliche Nutzung bereits erhobener Daten für andere Zwecke beabsichtigt ist, erfordert die Prüfung der Zulässigkeit eine vorherige Einschaltung der/des Datenschutzbeauftragten.

Ein Beteiligungskatalog mit erschöpfender Aufzählung aller Beteiligungstatbestände kann nicht genannt werden. Die Konsultierung der/des Datenschutzbeauftragten erstreckt sich z.B. von ihrer/seiner Mitwirkung bei der datenschutzkonformen Ausgestaltung von Geschäftsprozessen, Vordrucken und Verträgen bis hin zur Begleitung von Projekten, jeweils zur Überprüfung ihrer Datenschutzverträglichkeit. In Zweifelsfällen sollte die Frage, ob ein Beteiligungstatbestand gegeben ist, gemeinsam mit der/dem Datenschutzbeauftragten geklärt werden.

### **Zuständigkeit für die Beteiligung**

Für Verfahren und/oder Projekte, die ausschließlich im Jobcenter geplant oder betrieben werden, ist die/der Datenschutzbeauftragte des Jobcenters zuständig, da die Jobcenter eigene verantwortliche Stellen sind (vgl. § 50 Abs. 2 SGB II). Sie/er ist ferner für die Kontrolle und Verwendung der zentralen Verfahren der BA sowie für die Beratungs- und Kontrollfunktion hinsichtlich der Datenschutzangelegenheiten vor Ort zuständig. Verantwortliche Stelle für die vom Jobcenter zu nutzenden zentralen IT-Verfahren ist die BA (§ 50 Abs. 3 SGB II).

Der Mitarbeiterdatenschutz sowohl der im Jobcenter beschäftigten BA-Mitarbeiter/ innen als auch der kommunalen Mitarbeiter/innen gehört zum Zuständigkeitsbereich der/des benannten Datenschutzbeauftragten des Jobcenters.

### **Durchführung der Beteiligung**

Die Unterrichtung bzw. Information des/der Datenschutzbeauftragten erfolgt durch Übersendung der wesentlichen Planungsunterlagen oder eine zusammenfassende Darstellung über Inhalt und Stand des beabsichtigten Vorhabens. Der Umfang des Informationsmaterials sollte den Grundsätzen einer effektiven und effizienten Aufgabenerledigung entsprechen und sich auf wesentliche Inhalte beschränken.

Im Entscheidungsstadium erfolgt die Einschaltung der/des Datenschutzbeauftragten durch Mitzeichnung, wodurch ihre/seine Beteiligung, ihre/seine datenschutzrechtliche Zustimmung oder ggf. die abweichende Auffassung dokumentiert werden. Ohne die entsprechende Dokumentation ihrer/seiner rechtzeitigen Beteiligung und ihrer/seiner Stellungnahme ist eine Auftragserteilung nicht zulässig.

Bei komplexen bzw. fachspezifischen Sachverhalten ist ein/e fachkundige/r Mitarbeiter/in zu benennen, der/die als Ansprechpartner/in für die/den Datenschutz-beauftragte/n zur Verfügung steht.

### Zeitpunkt der Beteiligung

*Nach § 4g Abs. 1 S.3 Nr. 1 BDSG ist die/der Datenschutzbeauftragte über Vorhaben der automatisierten Verarbeitung personenbezogener Daten „rechtzeitig“ zu unterrichten. Diese gesetzliche Vorgabe wird nur dann gewahrt, wenn die/der Datenschutzbeauftragte ausreichend Zeit zur Stellungnahme hat und ihre/seine Stellungnahme die Planungen noch beeinflussen kann.*

*Unabhängig von den Beteiligungspflichten kann das Beratungsangebot der/des Datenschutzbeauftragten jederzeit in Anspruch genommen werden.*

### Rechte und Befugnisse des/der Datenschutzbeauftragten im Beteiligungsverfahren

Der/dem Datenschutzbeauftragten ist auf ihr/sein Verlangen bei der datenschutzrechtlichen Prüfung der angezeigten Maßnahmen oder des Verfahrens uneingeschränkt Auskunft zu erteilen. Ihr/ihm ist Einblick in sämtliche, die Maßnahme oder das Verfahren betreffenden Unterlagen zu gewähren. Außerdem hat sie/er jederzeit und unbeschränkt Zugang zu den jeweils verarbeiteten personenbezogenen Daten.

## Übersicht über die Übermittlungstatbestände des SGB X

- neben der Einwilligung nach § 67b Abs. 1 SGB X -

<b>Übermittlungszwecke, aufsteigend geordnet nach dem übermittlungsfähigen Datenumfang Übermittlungszweck</b>	<b>Übermittlungsfähiger Datenumfang</b>	<b>Besondere Übermittlungsbedingungen bzw. Voraussetzungen</b>	<b>Besondere Übermittlungsverfahren</b>
§ 68 Aufgaben der Polizeibehörden, der Staatsanwaltschaft und Gerichte, der Gefahrenabwehr und der Justizvollzugsanstalten oder Durchsetzung öffentlich-rechtlicher Ansprüche ab 600,-€	Vor- und Familienname, Geburtsdatum, Geburtsort, derzeitige Anschrift des Betroffenen sowie Name und Anschrift seines derzeitigen Arbeitgebers.	Übermittlung nur, soweit kein Grund zur Annahme besteht, dass schutzwürdige Belange des Betroffenen beeinträchtigt werden. Keine Übermittlungspflicht, wenn sich die ersuchende Stelle die Angaben auf andere Weise beschaffen kann.	Über Übermittlungsersuchen entscheidet der Leiter der ersuchten Stelle, sein allgemeiner Stellvertreter oder ein besonders bevollmächtigter Bediensteter.
§ 72 Schutz der inneren und äußeren Sicherheit	Wie obenstehend; zusätzliche frühere geführte Namen und Anschriften des Betroffenen sowie Namen und Anschriften früherer Arbeitgeber.	keine	Über Erforderlichkeit entscheidet ein vom Leiter der ersuchenden Stelle bestimmter Beauftragter, der die Befähigung zum Richteramt haben soll. Die oberste Bundes-/ Landesbehörde für ersuchende Stelle ist zu unterrichten. Bei ersuchter Stelle entscheidet Behördenleiter oder sein allg. Stellvertreter.
§ 73 Abs. 2 Übermittlung für die Durchführung eines Strafverfahrens bei Vergehen	Wie oben stehend; zusätzlich Angaben über erbrachte und demnächst zu erbringende Geldleistungen.	keine	Richterliche Anordnung erforderlich
§ 67e Bekämpfung von Leistungsmissbrauch und illegaler Beschäftigung	1. ob und welche Art von Sozialleistungen nach dem SGB oder Leistungen nach dem Asylbewerberleistungsgesetz bezogen wird, 2. bei welcher Krankenkasse versichert oder ob als Selbständige tätig, 3. ob und welche Art von Beiträgen nach diesem Gesetzbuch abgeführt und 4. ob und welche ausländischen Arbeitnehmer mit einer für ihre Tätigkeit erforderlichen Genehmigung und nicht zu ungünstigen Arbeitsbedingungen als vergleichbare deutsche Arbeitnehmer beschäftigt wurden	Nr. 1 an jeweils zuständigen Leistungsträger Nr. 2 bis 4 an jeweils zuständige Einzugsstelle	
§ 69 Erfüllung sozialer Aufgaben § 70 Durchführung des Arbeitsschutzgesetzes § 71 Erfüllung besonderer gesetzlicher Pflichten und Mitteilungsbefugnisse § 73 Nr. 1 Durchführung eines Strafverfahrens bei Verbrechen und Straftaten von erheblicher Bedeutung § 74 Verletzung der Unterhaltspflicht und Versorgungsausgleich § 75 Forschung und Planung	Alle für nebenstehende Zwecke erforderlichen Daten	§§ 70, 75 soweit nicht schutzwürdige Belange des Betroffenen beeinträchtigt werden oder das öffentliche Interesse, das Geheimhaltungsinteresse des Betroffenen erheblich überwiegt. § 75 Vorrangig zumutbar: Einholung der Einwilligung des Betroffenen oder Zweck anderweitig erreichbar.	§ 73 Richterliche Anordnung erforderlich. § 69 Abs. 1 Nr. 3, § 75 Vorherige Genehmigung durch die zuständige oberste Bundes-/Landesbehörde erforderlich.

Bei sämtlichen Übermittlungstatbeständen sind die einschlägigen Bestimmungen der §§ 76 und 77 SGB X zu beachten, und zwar § 76 Einschränkung der Übermittlungsbefugnis bei besonders schutzwürdigen personenbezogenen Daten, § 77 Einschränkung der Übermittlungsbefugnis über die Grenze. Außerdem ist der § 78 SGB X (Zweckbindung und

## Unterstützende Links

>>>HEGA 10/07 - 06 – Datenschutz in der Bundesagentur für Arbeit, Organisation des Datenschutzes, Aktualisierung und Zusammenfassung der Weisungen  
[http://www.baintern.de/nn\\_551462/zentraler-Content/A-08-Ordnung-und-Recht/HEGA/Dokument/HEGA-10-2007-VA-Datenschutz-in-der-BA,templateId=renderPrint,view=nav.html](http://www.baintern.de/nn_551462/zentraler-Content/A-08-Ordnung-und-Recht/HEGA/Dokument/HEGA-10-2007-VA-Datenschutz-in-der-BA,templateId=renderPrint,view=nav.html)

>>>HEGA 10/07 - 07 – Beachtung des Sozialdatenschutzes in den IT-Verfahren der BA  
[http://www.baintern.de/nn\\_398406/zentraler-Content/A-08-Ordnung-und-Recht/HEGA/Dokument/HEGA-10-2007-VA-Sozialdatenschutz-im-IT-Verfahren.html](http://www.baintern.de/nn_398406/zentraler-Content/A-08-Ordnung-und-Recht/HEGA/Dokument/HEGA-10-2007-VA-Sozialdatenschutz-im-IT-Verfahren.html)

>>>HEGA 03/10 - 02 – Vergabe von Berechtigungen im IT-Verfahren VerBIS  
[http://www.baintern.de/nn\\_551462/zentraler-Content/HEGA/2010/03/HEGA-03-2010-VA-Berechtigungen-VerBIS,view=nav.html](http://www.baintern.de/nn_551462/zentraler-Content/HEGA/2010/03/HEGA-03-2010-VA-Berechtigungen-VerBIS,view=nav.html)

>>>HEGA 09/12 – 02 – Vergabe von Berechtigungen im IT-Verfahren COSACH  
[http://www.baintern.de/nn\\_551462/zentraler-Content/HEGA/2012/09/HEGA-09-2012-VA-Berechtigungen-COSACH,view=nav.html](http://www.baintern.de/nn_551462/zentraler-Content/HEGA/2012/09/HEGA-09-2012-VA-Berechtigungen-COSACH,view=nav.html)

>>>E-Mail-Info SGB III vom 22.09.2009/ Geschäftsanweisung SGB II Nr. 29 vom 22.09.2009 - Beachtung des Sozialdatenschutzes bei der Integrationsarbeit und Anwendung von VerBIS und in der Jobbörse  
[http://www.baintern.de/nn\\_551462/zentraler-Content/Weisungen/E-Mail-Infos/2009/E-Mail-Info-2009-09-22,view=nav.html](http://www.baintern.de/nn_551462/zentraler-Content/Weisungen/E-Mail-Infos/2009/E-Mail-Info-2009-09-22,view=nav.html)

>>> VerBIS Arbeitshilfe - Sozialdatenschutz im Zusammenhang mit der Erfassung sensibler Daten und Veröffentlichung von Bewerberdaten in der JOBBÖRSE  
<http://www.baintern.de/zentraler-Content/A-04-Vermittlung/A-042-Vermittlung/Generische-Publikation/AH-VerBIS-Sozialdatenschutz.pdf>  
Geheimhaltungspflicht des Empfängers) zu beachten (Information des Datenempfängers)

Weitere Regelungen zum Datenschutz sind abrufbar unter:

<http://www.baintern.de/bund/generator/goto?id=363158>  
>>>Datenschutz – auch das noch

<http://www.baintern.de/bund/generator/goto?id=502056>  
>>> Arbeitshilfe Datenschutz in der BA