Arbeitsanweisung

Nr. 03/2010

jobcenter Berlin Tempelhof-Schöneberg

Geschäftszeichen:	II - 2081
Gültigkeit ab:	**12.07.2010**
Gültigkeit bis:	**unbefristet**
Verteiler:	**alle Mitarbeiter/innen**
letzte Aktualisierung:	**25.11.2011**

Datenschutz

Inhaltsverzeichnis

1. Datenschutz

Umgang mit personenbezogenen Daten

Die Beschäftigten müssen beim Umgang mit personenbezogenen Daten und Sozialdaten, die zum Schutz des Persönlichkeitsbereichs und der Privatsphäre des Bürgers bestehenden datenschutzrechtlichen Bestimmungen (Bundesdatenschutzgesetz, Sozialgesetzbücher II und X, Abgabenordnung u. ä.) sowie diesbezügliche Weisungen beachten. Hierzu gehören die Datenschutzbestimmungen der BA, die die Datenschutz- und Datensicherheits-konforme Aufgabenerledigung regeln.

Unterlagen mit personenbezogenen Daten

Unterlagen mit personenbezogenen Daten und Sozialdaten dürfen nur den dienstlich damit befassten Beschäftigten zugänglich gemacht werden und sind ansonsten unter Verschluss zu halten. Nach Dienstschluss sowie im Falle der Abwesenheit einer/eines Beschäftigten (Urlaub, Krankheit o.ä.) sind diese Unterlagen in verschließbaren Räumen oder in verschließbaren Behältnissen (Schränke, Schreibtische) unterzubringen, damit insbesondere amtsfremde Personen (z.B. Reinigungskräfte) keine Zugriffsmöglichkeit darauf haben. Nach Dienstschluss dürfen sich keine Unterlagen mit personenbezogenen Daten und Sozialdaten auf den Schreibtischen oder Ablagen befinden.

IKT

Die Informations- und Kommunikationstechnik der BA ermöglicht auch die Erstellung und Verarbeitung (Übermittlung, Speicherung u. ä.) persönlicher Dokumente. Mit Ausnahme sog. „privatdienstlicher“ Dokumente (z.B. Schreiben an den Personal-Service, Bewerbungen, Stellungnahmen in Haftungsverfahren) dürfen die Einrichtungen der Informations- und Kommunikationstechnik der BA nicht für private Zwecke genutzt werden. Einzelheiten, auch bezüglich des Zugriffs auf Dokumente im Rahmen der Ausübung der Dienst- und Fachaufsicht, regelt die Dienstvereinbarung IKT BA und Dienstvereinbarung über die Nutzung des Internets und anderer elektronischer Informations- und Kommunikationsdienste in der Berliner Verwaltung (Internet-DV).

2. Auskünfte

mdl. und tel. Auskünfte

Mündliche und telefonische Auskünfte sind höflich, erschöpfend, sachlich und klar zu geben. Kann eine Auskunft nicht erteilt werden, sind Auskunftssuchende an die zuständige Stelle zu verweisen. Am Telefon ist bei Auskünften, insbesondere aus Gründen des Datenschutzes, Zurückhaltung und besondere Vorsicht geboten. Je nach Lage des Falles sind Auskunftssuchende auf den schriftlichen Weg zu verweisen.

Aktenvermerk anfertigen bei der Erteilung von Auskünften

Grundsätzlich ist bei Erteilung von Auskünften ein Aktenvermerk anzufertigen. Bei besonders wichtigen Auskünften ist der Aktenvermerk der bzw. dem zuständigen Vorgesetzten zur Kenntnis vorzulegen. Auskünfte über Mitarbeiterinnen und Mitarbeiter sind der Geschäftsführung oder der von ihr beauftragten Stelle vorbehalten. Auskünfte an Polizei und Ermittlungsbehörden werden durch die Datenschutzbeauftragte /den Datenschutzbeauftragten ggf. nach Einschaltung des Fachbereiches erteilt (Anlage 1). Auskünfte an Zeitungen, Zeitschriften, Agenturen, Rundfunk und Fernsehen erteilen die Geschäftsführung, die Ansprechpartnerin / der Ansprechpartner für Presse und Öffentlichkeitsarbeit sowie von der Geschäftsführung ausdrücklich beauftragte Beschäftigte. Vom Ergebnis des Gesprächs ist die Geschäftsführung zu unterrichten. Journalistinnen und Journalisten, die das Jobcenter aufsuchen, sind zur Ansprechpartnerin / Ansprechpartner für Presse und Öffentlichkeitsarbeit zu begleiten.

3. E-Mail

E-Mail und Telefonie

Näheres siehe E-Mail-Verkehr und Arbeitsanweisung E-Mail-Versand, Telefonie.
Hinsichtlich der Schutzbedürftigkeit von Daten unterscheidet die IT-Sicherheitsrichtlinie 02 (unter IT-Sicherheitsrichtlinien im Intranet) fünf Schutzbedarfsklassen:

- Daten ohne Schutzbedarf (= Schutzbedarfsklasse 0) oder mit niedrigem Schutzbedarf (= Schutzbedarfsklasse 1 - z.B. Amts- und Dienstbezeichnungen, Mitgliederverzeichnisse, Geburtsjahr, Bankverbindung) dürfen ohne weiteres per E-Mail übermittelt werden
- Daten mit mittlerem, hohem oder sehr hohem Schutzbedarf (Schutzbedarfsklassen 2, 3 oder 4 – z.B. Daten über Kontostand, Einkommen, Gleitzeitdaten, dienstliche Beurteilungen, Beihilfe- oder Patientendaten, Zeugenadressen) dürfen aus Sicherheitsgründen generell nicht per E-Mail übermittelt werden, außer, wenn bei Daten der Schutzbedarfsklasse 2 (mittlerer Schutzbedarf) der Betroffene nachweislich in die Übermittlung eingewilligt hat. Die Verschlüsselungsmethoden des Office-Paketes sind hierbei jedoch verpflichtend zu nutzen.

Sicherheitsrichtlinien

Zu beachten sind ferner:

- die IT-Sicherheitsrichtlinie 05 – Nutzung von E-Mail
- die IT-Sicherheitsrichtlinie 01 – zur IT-Sicherheit von Geschäftsinformationen
- die IT-Sicherheitsrichtlinie 02 – Klassifizierung von Geschäftsinformationen

4. Posteingang

Verfahren bei Postein- und Postausgang

Das Verfahren für die Behandlung von Postein- und Postausgängen ist gesondert geregelt.

Folgende Eingänge werden ungeöffnet an den Adressaten weitergeleitet:

- Sendungen mit dem Zusatz "Persönlich", "Persönlich oder Vertreter" bzw. "Eigenhändig",
- Sendungen an die Geschäftsführung,
- Personalsachen ("P"),
- Sendungen, die als erstes den Namen in der Anschrift benennen.

5. Aussonderung von Altschriftgut und Datenschutzunterlagen

Aussonderung von Unterlagen

Unterlagen mit personenbezogenen Daten und Sozialdaten, die dienstlich nicht mehr benötigt werden, dürfen nicht mit dem normalen Papier- oder Restmüll entsorgt werden. Vielmehr sind hierfür ausschließlich sogenannte Datenschutzcontainer zu nutzen, deren Standorte aus der Anlage 2 zu entnehmen sind. Die Räume, in denen die Datenschutzcontainer vorgehalten werden, sind nach dem Verlassen zu schließen. Das Blockieren der Tür mittels Gegenständen ist aufgrund von Brandschutzvorschriften und datenschutzrechtlichen Gründen nicht gestattet.

Aussonderung von Altakten

Die Aussonderung von Altakten (gemäß Aktenplan) liegt in der Zuständigkeit der aktenführenden Bereiche. Die Aufbewahrungsfristen sind aus dem Aktenplan ersichtlich, die bei der Aussonderung der Altakten dienlich sind. Die Aussonderungsverzeichnisse sind anschließend dem Team 601 zuzuleiten, dort werden sie geführt. Für die Aussonderung können zusätzliche Datenschutzcontainer durch das Team 601 bereitgestellt werden.

Entsorgung von DVD's etc.

Nicht mehr benötigte „harte Datenträger“ (DVD, CD, USB-Sticks, Festplatten u. ä.) sind dem Team 601 zur datenschutzkonformen Vernichtung zu übergeben.

6. Ordnungswidrigkeiten

Vorgänge bei Verdacht von Leistungsmissbrauch oder Strafanzeigen

Alle Vorgänge, die einen Verdacht des Leistungsmissbrauchs oder eine Straftat begründen, sind mit Leistungsakte an das Team 641 zu übergeben.

Dieses entscheidet, ob nach Sachverhalt

- ein Bußgeldverfahren einzuleiten oder
- der Vorgang der Zollverwaltung zu übergeben oder
- der Vorgang an die Staatsanwaltschaft abzugeben ist.

7. Informationsfreiheitsgesetz (IFG)

IFG

Das Informationsfreiheitsgesetz ermöglicht jeder Bürgerin, jedem Bürger und jeder juristischen Person des Privatrechts den Zugang zu amtlichen Informationen des Bundes und des Landes, ohne dass besondere Antragsvoraussetzungen erfüllt sein müssen. Weitere Hinweise zur Verfahrensweise sind der HEGA 11/2006 – 15 – zu entnehmen. Anfragen werden durch die / den Datenschutzbeauftragte(n) des Jobcenter koordiniert

8. IT-Sicherheit / Informationssicherheit

Nutzung IKT

Bei der Erhebung, Verarbeitung und Nutzung von Informationen sowie der Nutzung der IT der BA sind die geltenden IT-Sicherheitsregelungen zu beachten.

Die Geschäftsführung stellt die erfolgreiche Umsetzung und Gewährleistung der IT-Sicherheit im eigenen Zuständigkeitsbereich auf der Basis zentraler Vorgaben sicher.

Die ganzheitliche IT-Sicherheitsorganisation ist mit HEGA 08/2007-18 und HEGA 12/2008-32 geregelt. Weitere Informationen bzw. Hinweise dazu siehe IT-Sicherheit.

9. IT-Sicherheitsverantwortlicher

IT-Sicherheitsverantwortliche

Die Aufgaben der/des IT-Sicherheitsverantwortlichen sind mit HEGA 12/2008 - 32 geregelt. Die Benennung der der /des IT-Sicherheitsverantwortlichen erfolgt durch die Geschäftsleitung.

10. Ansprechpartner

Ansprechpartner

Folgende Ansprechpartner wurden durch die Geschäftsleitung benannt.

Datenschutzbeauftragte, Ansprechpartnerin für Polizei und Ermittlungsbehörden:

e-Mail:
Jobcenter-Berlin-Tempelhof-Schoeneberg.Datenschutzbeauftragter@jobcenter-ge.de

Berlin, den 25.11.2011

Ingrid Wagener
Geschäftsführerin
Jobcenter Berlin Tempelhof-Schöneberg

Anlage 1

Berliner Beauftragter für Datenschutz und Informationsfreiheit

Datenübermittlung an Polizeibehörden durch das Jobcenter

Bei Anfragen der Polizei über Sozialdaten von Leistungsempfängern sind aus datenschutzrechtlicher Sicht folgende Punkte zu beachten:

1. In jedem Jobcenter ist ein zuständiger Mitarbeiter zu benennen, der über das jeweilige Ermittlungsersuchen entscheidet, vgl. § 68 Abs. 2 SGB X: Leiter der ersuchten Stelle, sein allgemeiner Stellvertreter oder ein besonders bevollmächtigter Mitarbeiter (evtl. Ansprechpartner für Datenschutz).

   Bei Anfragen der Polizeibeamten vor Ort sollen diese ausschließlich an den benannten Mitarbeiter verwiesen werden.

2. Es soll keine Datenübermittlung durch weitere Mitarbeiter/innen des Jobcenters (z.B. Sachbearbeiter/ zuständiger Arbeitsvermittler) erfolgen.

3. Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle gemäß § 67 d Abs. 2 Satz 1 SGB X.

4. Auskunftsersuchen sind nur in begründeten Einzelfällen unter Benennung der jeweiligen Rechtsgrundlage zulässig (Jobcenter hat nicht die Funktion von Ersatzmeldebehörden).

5. Um die Zulässigkeit der Datenübermittlung prüfen zu können, muss das Ersuchen der Polizei im Regelfall schriftlich erfolgen. Die auskunftsuchenden Beamten sind auf den Schriftweg zu verweisen.

6. Bei Anfragen von Polizeibeamten vor Ort bei dem zu benennenden zuständigen Mitarbeiter des Jobcenters können Daten nur in begründeten Ausnahmefällen direkt übermittelt werden. Es soll keine Auskunftserteilung über verschiedene Leistungsempfänger gleichzeitig erfolgen.

7. Eine Auskunft kann nur nach Legitimation durch Vorlegen des Dienstausweises erteilt werden.

8. Als Norm zur Datenübermittlung kommen insbesondere die §§ 68, 73 und 69 Abs. 1 Nr. 2 SGB X in Betracht

   Im Rahmen des § 68 SGB X dürfen ausschließlich folgende Daten übermittelt werden: Name, Vorname, Geburtsdatum, Geburtsort, derzeitige Anschrift des Betroffenen, derzeitiger oder zukünftiger Aufenthalt (darunter fallen auch zukünftige Vorsprache-Termine beim Jobcenter), Namen und Anschriften der derzeitigen Arbeitgeber.

   Weitere Sozialdaten dürfen gemäß § 73 SGB X ausschließlich aufgrund einer richterlichen Anordnung weitergegeben werden.

   Datenübermittlung nach § 69 Abs. 1 Nr. 2 SGB X bilden die Ausnahme und sind daher besonders zu prüfen.

9. Die Auskunftsersuchen durch die Polizei (auch bei verweigerter Datenübermittlung) sind zwingend zu dokumentieren (Datum, Name des Beamten, Dienstnummer, Zweck der Datenabfrage, benannte Rechtsgrundlage, Name des Betroffenen, evtl. Zeugen etc.).

10. Falls Unsicherheit über die Zulässigkeit der Datenübermittlung besteht, sollten Daten zunächst nicht übermittelt werden; der zuständige Mitarbeiter kann sich zwecks Beratung an den Berliner Beauftragten für Datenschutz und Informationsfreiheit wenden.

Anlage 2

Raum	Eingangszone II (nähe Platz 13)
Raum	AAS (vor dem Raum 8)
Raum	1066
Raum	2000
Raum	2070
Raum	3000
Raum	3070
Raum	4020
Raum	4067
Raum	4107