jobcenter
Landau-Südliche Weinstraße

Geschäftsanweisung 04 / 2018

Landau, den 20.09.2018
Verteiler: alle Mitarbeiterinnen und Mitarbeiter des Jobcenters

Datenschutz

Geschäftszeichen:
II-1500

---

1. Einleitung – Datenschutz ist Persönlichkeitsschutz

Ziel des Datenschutzes ist es, die einzelne Person (hier: Kunden) davor zu schützen, dass ihre Daten in unzulässiger Weise verwendet werden.
Grundsätzlich hat jeder Einzelne das Recht, zu bestimmen, wem er seine persönlichen Daten preisgibt. Jeder ist „Herr seiner Daten". Darüber hinaus hat jeder Einzelne grundsätzlich einen Anspruch darauf, zu wissen, welche Daten über ihn bei welcher Stelle gespeichert sind oder auf sonstige Weise verarbeitet werden. Auf Wunsch können ihm Kopien der gespeicherten Unterlagen ausgehändigt werden.

Achtung: Gutachten des Berufspsychologischen Service dürfen nur von diesem an den Kunden weitergegeben werden!
Das Gleiche gilt für Gutachten des Ärztlichen Dienstes, soweit Teil A betroffen ist. Teil B (Sozialmedizinische Stellungnahme) darf ausgehändigt werden, soweit der Ärztliche Dienst die Eröffnung dem Fachbereich übertragen hat.

Alle Beschäftigten des Jobcenters Landau - Südliche Weinstraße haben beim Umgang mit personenbezogenen Daten die zum Schutz des Persönlichkeitsbereichs und der Privatsphäre des Bürgers erlassenen datenschutzrechtlichen Bestimmungen, insbesondere des Sozialgesetzbuches (SGB), der Datenschutz-Grundverordnung (DSGVO), des Bundesdatenschutzgesetzes (BDSG neu) und des Informationsfreiheitsgesetzes (IFG) sowie die diesbezüglichen Weisungen zu beachten.

2. Definition

„Personenbezogene Daten" sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind (Art. 4 Nr. 1 DSGVO, § 46 Nr. 1 BDSG neu). Diese Daten sind besonders schützenswert; sie unterliegen den Regelungen der DSGVO und des BDSG neu. Allgemein gilt, dass personenbezogene Daten nur dann erhoben, verarbeitet oder genutzt werden dürfen, wenn dies durch gesetzliche Bestimmungen oder eine Einwilligung der betroffenen Person legitimiert ist.

3. Verarbeitung von Daten

Grundsätze für die Verarbeitung personenbezogener Daten enthalten Art. 5 DSGVO, § 47 BDSG neu. Dies sind insbesondere:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit

Insoweit dürfen Daten nur für die Zwecke verarbeitet und genutzt werden, für die sie erhoben worden sind. Zudem dürfen sie hinsichtlich Art, Umfang und Dauer nur insoweit erhoben, verarbeitet und genutzt werden, wie dies zur Erledigung der jeweiligen gesetzlichen Aufgabe unabdingbar notwendig ist. Insbesondere ist von den Möglichkeiten der Anonymisierung und **Pseudonymisierung** Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Die Anlagen eins und zwei der Arbeitshilfe – Hinweise zum Aufbau und Führen einer Leistungsakte sind zu beachten (Inhalt einer Leistungsakte). So sind beispielsweise keine Kopien von Ausweisdokumenten, Bankkarten, Krankenkassenkarten, Sozialversicherungsausweisen zur Akte zu nehmen.
Weiterhin müssen die technischen und organisatorischen Maßnahmen getroffen werden, die erforderlich sind, um die Ausführung der datenschutzrechtlichen Bestimmungen und Anforderungen zu gewährleisten (Art. 32 DSGVO).

4. Aufbewahrung von Daten

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.

5. Übermittlung von Daten

Regelungen zur Übermittlung personenbezogener Daten enthält § 25 BDSG neu. Die Übermittlung personenbezogener Daten durch öffentliche Stellen an öffentliche Stellen ist zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Dritten, an den die Daten übermittelt werden, liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Verarbeitung nach § 23 BDSG neu zulassen würden.

Mailverkehr mit personenbezogenen Daten ist ausschließlich in verschlüsselter Form zulässig. Ist eine Verschlüsselung nicht möglich, darf nicht per Mail kommuniziert werden.

Im Rahmen der Integration ist vor der Übermittlung von Sozialdaten aus dem Profiling unbedingt die Einwilligung der Kundin/des Kunden erforderlich. Dies ist durch Betätigen der entsprechenden Kontrollfelder in der Schlüsselgruppe „Rahmenbedingungen“ in VerBIS zu dokumentieren.

5. Gesetzliche Grundlagen und weitere Informationen

Gesetzliche Grundlagen sind insbesondere die DSGVO, das BDSG neu und andere gesetzliche Vorschriften über den Datenschutz, z.B. aus dem SGB X.

Die der GA als Anlage 1 beigefügte Informationen zur Datenerhebung nach Art. 13 und 14 DSGVO für den SGB II-Bereich ist zu beachten.

6. Vernichtung von Daten

Personenbezogene Daten, die zur Vernichtung freigegeben sind, müssen sicher gelöscht bzw. vernichtet werden. Datenschutzwürdige Unterlagen in Papierform müssen speziell entsorgt werden und in so genannte Datenschutzcontainer gegeben werden.
Datenschutzrechtlich relevante Papiervorgänge sind von den Mitarbeiterinnen und Mitarbeitern am Arbeitsplatz zu sammeln und einmal täglich in den aufgestellten Datenschutzcontainern zu entsorgen. Die jeweiligen Standorte der Datenschutzcontainer werden per Mail bekannt gegeben.

7. Besonderheiten

Bei Amtshilfeersuchen von Strafverfolgungsbehörden ist es zulässig, den Vorsprachetermin eines Kunden unter bestimmten Voraussetzungen zu übermitteln. Die Entscheidung hierüber obliegt der Geschäftsführerin/dem Geschäftsführer, seinem/ihrem allgemeinen Stellvertreter oder einem hierfür besonders bevollmächtigten Bediensteten. Hierzu wird auf die HEGA 06/09 – 11 verwiesen.

8. Verfahren bei unrechtmäßiger Kenntniserlangung von Sozialdaten

Im Falle einer Verletzung des Schutzes personenbezogener Daten ist unverzüglich und möglichst binnen 72 Stunden, nachdem die Verletzung bekannt wurde, die zuständige Aufsichtsbehörde (BMAS) sowie die Bundesbeauftragte für Datenschutz und Informationsfreiheit zu informieren. Regelungen dazu enthält die Weisung 201805012 vom 23.05.2018 – Meldepflicht bei Verletzung des Schutzes von personenbezogenen Daten. Die Mitarbeiterin bzw. der Mitarbeiter, dem die Datenschutzpanne bekannt wird, informiert deshalb sofort die Datenschutzbeauftragte oder die Geschäftsführung über den Sachverhalt. Von der Geschäftsführung wird entschieden, welche weiteren Schritte einzuleiten sind (Information der Zentrale, bei Fehlkuvertierung Information Postdienstleister etc.). Regelungen enthalten Art. 33 und 34 DSVGO, § 83a SGB X sowie die §§ 65, 66 BDSG neu.

9. Beteiligung

Der Personalrat und die Gleichstellungsbeauftragte wurden beteiligt

10. Inkrafttreten

Diese Geschäftsanweisung tritt mit dem Tag der Veröffentlichung in Kraft

gez.
Geschäftsführer

gez.
Beauftragte für den Datenschutz