

# Jobcenter Intern

Jobcenter Region Hannover



Ausgabe/Aktenzeichen 06/2017

Veröffentlicht: 27.11.2017, aktualisiert 28.12.2018

## Dienstanweisung

Verfasser: Behördliche/r Datenschutzbeauftragte/r (bDSB)

## Melde- und Benachrichtigungspflichten bei Datenschutzverletzungen

### Inhalt

1. Rechts- und Weisungslage.....	2
2. Umsetzung und grundsätzliche Verantwortlichkeiten.....	2
2.1 Weitergehende Aspekte bei Fehlversendungen von Dokumenten .....	3
3. Begriffserläuterungen .....	4

## 1. Rechts- und Weisungslage

Das Jobcenter Region Hannover verarbeitet für die Erbringung der Aufgaben nach dem Zweiten Buch Sozialgesetzbuch (SGB II) im großen Umfang personenbezogene Daten. Einerseits werden zur Erbringung der Leistungen nach dem SGB II personenbezogenen Daten der Leistungsberechtigten verarbeitet und andererseits die Daten der Beschäftigten für die Personalverwaltung. Das Jobcenter Region Hannover ist damit für die Einhaltung der rechtlichen Bestimmungen zur Datenverarbeitung verantwortlich (Artikel 4 Europäische Datenschutzgrundverordnung in Verbindung mit § 50 Absatz 2 Zweites Buch Sozialgesetzbuch – SGB II und § 3 Bundesdatenschutzgesetz – BDSG).

Seit Wirksamkeit der DSGVO am 25.05.2018 müssen alle Verletzungen des Schutzes personenbezogener Daten („Datenschutzpannen“) binnen 72 Stunden nach Kenntnisnahme bei den Aufsichtsbehörden (Bundesministerium für Arbeit und Soziales und Bundesbeauftragte für den Datenschutz und die Informationsfreiheit) gemeldet werden (Artikel 33 DSGVO in Verbindung mit § 83a SGB X). Dazu gehören auch Datenschutzverletzungen, die durch sogenannte Auftragsverarbeiter des Jobcenters verursacht worden sind. Darüber hinaus sind die betroffenen Personen über den Vorfall zu benachrichtigen (Artikel 34 DSGVO in Verbindung mit 83a SGB X), sofern die Datenschutzverletzung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten der betroffenen Personen zur Folge hat.

Für die zentral verwalteten Verfahren der Informationstechnik (z.B. STEP, VerBIS, ALLEGRO) ist in datenschutzrechtlicher Hinsicht die Bundesagentur für Arbeit (BA) ebenso verantwortlich, wie für die vom Jobcenter Region Hannover eingekauften Dienstleistungen (z.B. zentrale Poststelle, Service Center). Soweit Datenschutzverletzungen auf Funktionen der zentral verwalteten Informationstechnik (§ 50 Absatz 3 SGB II) oder den Dienstleistungen der BA (§ 44b Absatz 4 und 5 SGB II) zurückzuführen sind, ist die behördliche Datenschutzbeauftragte der BA zu informieren ([Weisung 201805012 vom 23.05.2018](#)).

## 2. Umsetzung und grundsätzliche Verantwortlichkeiten

Zunächst sind zwei Fallgestaltungen zu unterscheiden, nach denen sich die weitere Vorgehensweise bestimmt:

- a) **Datenschutzverletzungen deren Ursachen auf Funktionen der zentralen Informationstechnik oder Dienstleistungen der BA beruhen**, werden von den jeweils zuständigen Standorten/Fachbereichen des Jobcenter Region Hannover gemäß der o.g. Weisung innerhalb von zwei Arbeitstagen nach Kenntnisnahme mittels Meldebogen per E-Mail verschlüsselt an [Zentrale.JDC-Datenschutz@arbeitsagentur.de](mailto:Zentrale.JDC-Datenschutz@arbeitsagentur.de) gemeldet.

Die behördliche Datenschutzbeauftragte (bDSB) des Jobcenter Region Hannover ist parallel per Cc [Jobcenter-Region-Hannover.Datenschutz@jobcenter-ge.de](mailto:Jobcenter-Region-Hannover.Datenschutz@jobcenter-ge.de) zu informieren. Dies kann mithilfe der **lokalen BK-Textvorlage „Meldung Datenschutzverletzung an die Zentrale (JDC)“** unter dem Ordner Alg II umgesetzt werden.

**b) Datenschutzverletzungen, die in Verantwortung des Jobcenters Region Hannover oder dessen Auftragsverarbeiter entstanden sind**, sind durch die jeweilig zuständigen Standorte/Fachbereiche vor Ablauf von 72 Stunden nach Kenntnisnahme, an die bDSB des Jobcenter Region Hannover [Jobcenter-Region-Hannover.Datenschutz@jobcenter-ge.de](mailto:Jobcenter-Region-Hannover.Datenschutz@jobcenter-ge.de) zu melden. Dabei müssen mindestens folgende Informationen enthalten sein:

- Datum und Zeitpunkt der Kenntnisnahme der Datenschutzverletzung durch das Jobcenter Region Hannover,
- Beschreibung der Datenschutzverletzung (wie ist es passiert, wieviel betroffene Personen, welche Daten wurden offenbart),
- Beschreibung der möglichen Risiken oder bereits eingetretenen Folgen für die betroffenen Personen,
- Hinweis, ob die betroffene Person informiert wurde (bei hohem Risiko für die Rechte und Freiheiten zwingend erforderlich) und
- Beschreibung oder Vorschläge von Maßnahmen zur Behebung der Fehlerquelle oder zur Abmilderung der Auswirkungen der Datenschutzverletzungen.

Für die Meldung ist die lokale **BK-Textvorlage „Meldung Datenschutzverletzung Intern“** unter dem Ordner Alg II zu nutzen. Von der bDSB wird die Meldung an die Aufsichtsbehörden ([arbeitsgruppe12b@bfdi.bund.de](mailto:arbeitsgruppe12b@bfdi.bund.de), [lla1@bmas.bund.de](mailto:lla1@bmas.bund.de)) weitergeleitet.

## **2.1 Weitergehende Aspekte bei Fehlversendungen von Dokumenten**

Bei fehlgeleiteter Post ist durch die Beschäftigten sicher zu stellen, dass diese Dokumente vom unberechtigten Empfänger an das Jobcenter Region Hannover zurückgegeben werden. Alternativ ist auf die datenschutzgerechte Vernichtung der Dokumente hin zu wirken. Zudem ist die Post der/dem rechtmäßigen Empfänger/in (erneut) zuzusenden.

Es ist in den jeweiligen Standorten sicher zu stellen, dass Rechtsnachteile für die Betroffenen, z.B. in Form von Sanktionen durch einen verpassten Termin oder Versagung aufgrund fehlender Mitwirkung, durch entsprechende Information an die beteiligten Fachbereiche unbedingt vermieden werden!

### 3. Begriffserläuterungen

- **Personenbezogene Daten** sind alle Informationen, die sich auf eine Person beziehen oder mit denen direkt oder indirekt mit weiteren Hilfsmitteln auf eine bestimmte Person geschlossen werden kann, also auch Kundennummern, Personalnummern etc. (Artikel 4 Nr. DSGVO). „**Besondere personenbezogene Daten**“ sind Angaben, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit oder die Verarbeitung von genetischen und biometrischen Daten zur eindeutigen Identifizierung sowie Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer Person hervorgehen (Artikel 9 DSGVO).
- Ein **Risiko für die Rechte und Freiheiten** einer Person kann in physischer, materieller als auch immaterieller Hinsicht vorliegen. Stichworte für Risiken: Diskriminierung, Identitätsdiebstahl, finanzieller Verlust, Rufschädigung, unbefugter Zugriff auf gespeicherte Daten, erhebliche wirtschaftliche oder gesellschaftliche Nachteile. In der Praxis sind nachfolgende Beispiele denkbar:  
Einem Beschäftigten wird der mobile Arbeitsplatz gestohlen oder eine Akte ist unauffindbar (→ unzulässiger Zugriff auf Daten möglich). Ein Dritter erhält die Leistungsbescheide eines Kunden und trägt möglicher Weise diese Information in das soziale Umfeld weiter (→ Rufschädigung). Ein Arbeitgeber tritt kurzfristig von einem Beschäftigungsverhältnis zurück, weil er von einer chronischen Erkrankung des Bewerbers erfahren hat (→ Diskriminierung, ggf. auch finanzieller Verlust).
- Bei der **Risikoeinschätzung** ist eine Prognoseentscheidung der Eintrittswahrscheinlichkeit von negativen Folgen für die betroffene Person zu treffen. Von einem hohen Risiko ist z.B. immer auszugehen, wenn besondere personenbezogene Daten betroffen sind. Dies kann in der Praxis beispielsweise sein, wenn ein ärztliches Gutachten einem unberechtigten Dritten zur Kenntnis gelangt. Ein „normales“ Risiko besteht, wenn eine Einladung mit dem Standardtext an einen falschen Empfänger übersandt wird. Dass ein Risiko für die Rechte und Freiheiten der betroffenen Person bei einer Datenschutzverletzung gänzlich ausgeschlossen werden kann, wird in der Praxis nahezu nie zu prognostizieren sein.

- **Auftragsverarbeiter** sind Dienstleister, die für das Jobcenter Aufgaben übernehmen und dabei mit personenbezogenen Daten arbeiten, wie z.B. die Vernichtung von Datenmüll durch einen Entsorger oder das Versenden von Informationsschreiben an Leistungsberechtigte durch eine externe Druckerei. Maßnahme- und Bildungsträger (§ 16 Abs. 1 Satz 2 Nr. 2 SGB II i. V. m. § 45 SGB III, § 16 Abs. 1 SGB II i. V. m. §§ 81ff. SGB III) sind datenschutzrechtlich eigenverantwortlich und stellen keine Auftragsverarbeiter dar. Dienstleister, deren Aufgabenschwerpunkt nicht im Zusammenhang mit der Datenverarbeitung stehen (z.B. Sicherheitsdienst, Reinigungsdienst), werden zwar auf das Datengeheimnis verpflichtet, stellen aber ebenfalls keine Auftragsverarbeiter dar.
- **Maßnahmen zur Behebung der Fehlerquelle** können aus unterschiedlichen Blickwinkeln und Ebenen kommen. Der Regelung in der DSGVO geht es darum, dass Datenschutzverletzungen nicht nur gemeldet werden, sondern die Verursacher auch gleichzeitig dafür sorgen, dass sich diese Fehler nicht wiederholen. Im Wirkungskreis der operativen Führungskräfte sind z.B. folgende Maßnahmen denkbar: Beschäftigte für die Einhaltung datenschutzrechtlicher Bestimmungen sensibilisieren, falsche Handlungsweisen im Arbeitsalltag thematisieren/abstellen, Qualifizierungsdefiziten entgegenwirken, Arbeitsabläufe umstellen. **Abmilderung der Auswirkungen von Datenschutzverletzungen** können zum Beispiel erzielt werden, wenn ein ungewollt bekannt gewordenes Passwort gesperrt/geändert wird oder der unberechtigte Empfänger eines Briefes gebeten wird, das Schreiben an das Jobcenter zurück zu senden.

Der Geschäftsführung obliegt es, die entsprechenden Rahmenbedingungen zu schaffen, z.B. Qualifizierungen zu fördern, die Verträge mit Auftragsverarbeitern entsprechend zu gestalten, Dienstanweisungen zu erlassen oder zu verändern, die Diensträume datenschutzkonform auszustatten bzw. zu gestalten. Soweit es also um Sachverhalte geht, die nicht vor Ort von den operativen Bereichen beeinflusst werden können, müssen entsprechende Hinweise an die Geschäftsführung weitergegeben werden, damit von dort aus Maßnahmen ergriffen werden können.