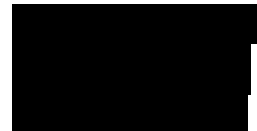



Jobcenter Oberhausen  
Geschäftsführung  
Marktstraße 31  
46045 Oberhausen

nachrichtlich:  
Bundesagentur für Arbeit  
Stabsstelle Datenschutz  
Regensburger Straße 104  
90478 Nürnberg

nachrichtlich:  
Bundesministerium für Arbeit und Soziales  
Referat IIc1  
Wilhelmstraße 49  
10117 Berlin



Telefon: +49 228 997799 

E-Mail:  
Referat15@bfdi.bund.de

Aktenz.:   
(bitte immer angeben)

Dok.: 

Anlage:

Bonn, 05.02.2025

## Datenschutzrechtliche Kontrolle im Jobcenter Oberhausen

Sehr geehrte Damen und Herren,

im Rahmen meiner Zuständigkeit gemäß den Artt. 55 Abs. 1, 57 Abs. 1 lit. a) sowie 58 Abs. 1 lit. b) Datenschutzgrundverordnung (DSGVO) und den §§ 9 Abs. 1 Satz 1, 14 Abs. 1 Nr. 1 Bundesdatenschutzgesetz (BDSG) habe ich mit Schreiben vom 14. Dezember 2023 eine datenschutzrechtliche Kontrolle auf schriftlichem Wege durchgeführt. Das Jobcenter Oberhausen (nachfolgend Jobcenter) wurde für diese Kontrolle ausgewählt. Gegenstand der Kontrolle war eine App des Jobcenters für mobile Endgeräte (Jobcenter App).

Sie wurden gebeten, von mir gestellte Fragen zu diesem Themenbereich vollständig, detailliert und nachvollziehbar zu beantworten und die Antworten – soweit möglich – durch schriftliche Nachweise zu belegen. Für die Beantwortung meiner Fragen mit Schreiben vom 19. Februar 2024 danke ich Ihnen.

Weitere Sachverhalte außerhalb des oben genannten Kontrollgegenstandes wurden nicht geprüft.

## **1. Ergebnis meiner Kontrolle:**

Im Zuge der fortschreitenden Digitalisierung begrüße ich ausdrücklich das digitale Angebot in Form der Jobcenter App des Jobcenters. Die Einführung dieser Anwendung stellt einen bedeutenden Schritt hin zu einer modernen und zeitgemäßen Kommunikation mit den Kunden dar.

Die App hat die Vorteile, dass sie viele Anliegen und Kommunikationswege erheblich vereinfacht. Kunden können problemlos und schnell auf wichtige Informationen zugreifen und Unterlagen digital einreichen. Dies spart nicht nur Zeit, sondern erhöht auch die Effizienz der Bearbeitung. Auch die Möglichkeit, flexibel und unabhängig von Ort und Zeit mit dem Jobcenter in Kontakt zu treten, entspricht den Anforderungen einer digital vernetzten Gesellschaft.

Im Ergebnis hat meine Kontrolle einige datenschutzrechtliche Defizite der App aufgezeigt. Diese sind im Einzelnen unter 3. (rechtliche Bewertung) dieses Kontrollberichtes aufgeführt. Da die App mit Einführung der Jobcenter-App der Bundesagentur vom Jobcenter seit dem 14.01.2025 nicht mehr betrieben wird, hat sich eine Behebung dieser Defizite erledigt. Meine Feststellungen bitte ich insofern im Sinne einer Sensibilisierung für datenschutzrechtliche Vorgaben bei künftigen Digitalisierungsvorhaben, des Jobcenters, zu denen ich Sie im Übrigen gerne berate, zu verstehen.

## **2. Sachverhalt:**

Die Kontrolle umfasste allgemeine Fragen zur Jobcenter App, zur Funktionsweise, zum Datenschutzmanagement und zu den Betroffenenrechten im Rahmen der App. Die Prüfung fand zu dem Zeitpunkt statt, als die App vom Jobcenter noch betrieben wurde. Auf diesen Zeitpunkt beziehen sich die folgenden Ausführungen.

Das Jobcenter bot seine App seit Mai/Juni 2020 zur Nutzung an. Mit der App konnten Kunden auf dem Smartphone bzw. Tablet Dienstleistungen des Jobcenters nutzen. Hierzu gehörten die Einreichung von Unterlagen, die Terminvereinbarung, ein Mietpreisprüfer sowie weitere Formularanträge. Mit Stand Februar 2024 wurde die App für das mobile Betriebssystem Android 3150 Mal und für iOS 9630 Mal heruntergeladen. Sämtliche Anliegen der Bürgerinnen und Bürger konnten allerdings auch ohne die App erledigt werden.

Es wurde des Weiteren folgender Sachverhalt bezüglich der App festgestellt:

## 1. Jobcenter App allgemein

Um die App für mobile Geräte mit dem Betriebssystem Android zu nutzen, musste ein Google-Account vorhanden sein, um die App über den Google Play Store beziehen zu können. Weitere Bezugsquellen der Android App bot das Jobcenter nicht an. Für iOS musste ein Apple-Account vorhanden sein, um die App über den Apple App Store beziehen zu können.

Beim Öffnen der App erschien ein Dialog. Darin wurde gefragt, ob der Nutzer mit den Datenschutzbestimmungen und Nutzungsbedingungen der App einverstanden ist. Der Dialog enthielt aufrufbare Links zu den Dokumenten. Mit den Buttons „Abbruch“ und „Okay“ konnte eine Auswahl getroffen werden. Durch Tätigen von „Abbruch“ schloss sich die App, während durch Betätigen von „Okay“ die Nutzung der App fortgesetzt und von einer Einwilligung ausgegangen wurde.

## 2. Funktionsweise

Es lag ein Verzeichnis von Verarbeitungstätigkeiten (VVT) für die App vor, zuletzt in der Version vom 21.02.2024.

Den Zweck für die Datenverarbeitung gab das Jobcenter in dem Dokument „Smartphone-App 2.0“ mit "Betrieb einer Smartphone-App für die Plattformen iOS (Apple) und Android (Google).Bereitstellung aller Online-Services auf einem mobilen Endgerät" an.

Die Auflistung der technisch-organisatorischen Maßnahmen gemäß Art. 32 DSGVO erfolgte im VVT-Eintrag. Es wurde die Transportverschlüsselung (SSL, SMIME) und die Existenz eines Berechtigungskonzepts genannt.

Das Jobcenter bediente sich des Dienstleisters und Auftragsverarbeiters [REDACTED] zum Betrieb der Server des Jobcenters. Das Rechenzentrum wurde vom Unterauftragsverarbeiter [REDACTED] betrieben. Hierüber lief die Website sowie die App. Es liegt eine Vereinbarung zur Auftragsdatenverarbeitung gemäß Art. 28 Abs. 3 DSGVO vor, die seit dem 25.05.2018 in Kraft war.

Zur Übertragung der Daten von der App zum Jobcenter wurde ein Gateway-Server aufgesetzt. Die Daten wurden per Hypertext Transfer Protocol Secure (HTTPS) an den Server des Auftragsverarbeiters [REDACTED] geschickt und von dort als verschlüsselte (S/MIME) E-Mail an das Jobcenter Postfach versendet. Demnach wurden die übermittelten Daten beim Auftragsverarbeiter [REDACTED] sowie bei dessen Unterauftragsverarbeiter im Klartext verarbeitet.

Nachdem das Jobcenter die Daten, die es von den Nutzern der App in Form einer E-Mail erhielt, empfangen hatte, wurden diese nach Erledigung von den zuständigen Mitarbeitern gelöscht. Weitere Regelungen hierzu waren nicht vorhanden. Informationen darüber, ob und wann die Protokolldateien, die im Rahmen der Verwendung der App beim Auftragsverarbeiter anfallen, gelöscht werden, fehlten.

In Punkt 10 der Datenschutzhinweise zur Smartphone-App wurde die Funktion von Push-Benachrichtigungen beschrieben. Beim erstmaligen Start der App wurde der Nutzer nach der Erlaubnis/Berechtigung gefragt, ob er Push-Benachrichtigungen erhalten möchte. Nach Zustimmung wurden "anonymisierte" Token von Google/Apple generiert, um damit Push-Benachrichtigungen an das Gerät zu senden. Die Zustimmung konnte vom Nutzer jederzeit in den Systemeinstellungen revidiert werden.

Durch die Nutzung der Push-Benachrichtigungs-Dienste von Google/Apple erfuhren diese Unternehmen, dass ein Nutzer die App des Jobcenters nutzt, sowie die Metadaten der Push-Nachrichten wie z.B. den Zeitpunkt an dem eine Nachricht übertragen wurde. Somit konnten Rückschlüsse auf die Aktivität der Nutzer gezogen werden.

### 3. Datenschutzmanagement

Das Jobcenter hatte keine Datenschutzfolgenabschätzung für die App vorgenommen. Es war der Ansicht, dass die im Kontext der Smartphone-App nebst angrenzenden technischen Systemen und Services verarbeiteten personenbezogenen Daten eine Datenschutzfolgenabschätzung nicht erforderlich machen. Zudem ging es davon aus, dass kein hohes Risiko für die Verarbeitung von Sozialdaten bestand.

Das Jobcenter bediente sich des Dienstleisters [REDACTED] zum Betrieb der Server des Jobcenters. Das Rechenzentrum wurde vom Unterauftragsverarbeiter [REDACTED] betrieben. Hierüber lief die Website sowie die App. Es lag eine Auftragsverarbeitung gemäß Art. 28 DSGVO vor. Laut Aussage des Jobcenters wurde die Vereinbarung zur Auftragsverarbeitung nur vorsorglich geschlossen, da die Daten ausschließlich in verschlüsselter Form über die Server transportiert wurden.

Der Auftragsverarbeiter wurde vom Jobcenter nicht selber kontrolliert. Es fand aber ein regelmäßiger Austausch mit ihm statt. Das Jobcenter hatte nicht angegeben, ob die Auftragsverarbeitung der Rechts- und Fachaufsicht angezeigt wurde.

### 4. Betroffenenrechte

Das Jobcenter gab an verschiedenen Stellen unterschiedliche Rechtsgrundlagen für die Verarbeitung der personenbezogenen Daten im Rahmen der App an: Als Rechtsgrundlage für die Verarbeitung der Daten in der App nannte es in seiner Antwort an mich Art. 6 Abs. 1 lit. a DSGVO (Einwilligung). Im aktuellen VVT der App war als Rechtsgrundlage neben Einwilligung zusätzlich "berechtigtes Interesse" angegeben. Diese Angabe fand sich auch in den Datenschutzhinweisen zur Smartphone-App wieder. Hier wurden unter Punkt 13 als Rechtsgrundlagen "6 Abs. 1 lit. a DSGVO", sowie "6 Abs. 1 lit. f DSGVO" genannt.

Eine Differenzierung, für welche Verarbeitung welche Rechtsgrundlage herangezogen wird, erfolgte durch das Jobcenter nicht.

In den Datenschutzhinweisen zur Smartphone-App wurde Art. 6 Abs. 1 lit. a) DSGVO im Zusammenhang mit der Erteilung von App-Berechtigungen für den Zugriff auf Kamera, Dateisystem und Kalender genannt.

Eine Speicherung von Logdaten erfolgte auf Grundlage von berechtigten Interessen im Sinne des Art. 6 lit. f) DSGVO.

Die Datenverarbeitung durch das Jobcenter Oberhausen stützte sich "insbesondere" auf Art. 6 Abs. 1 lit. c) DSGVO i.V.m. weiteren spezialgesetzlichen Regelungen sowie Art. 6 Abs. 1 lit. a) DSGVO, soweit die betroffene Person ihre Einwilligung erteilt hatte.

In Punkt 5 der Datenschutzhinweise zur Smartphone-App wurde die Verarbeitung von IP-Adressen nicht genannt.

In Punkt 7 der Datenschutzhinweise zur Smartphone-App gab das Jobcenter an, dass die folgenden Funktionen die App auch ohne Datenerhebung genutzt werden konnten: Veranstaltungskalender, News-Feed, Mietpreisprüfer, Anzeige externer Webinhalte des Jobcenters.

### **3. Rechtliche Bewertung**

Gemäß § 50 Abs. 4 S. 3 Sozialgesetzbuch Zweites Buch (SGB II) ist die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) für die Datenschutzaufsicht über das Jobcenter als gemeinsame Einrichtung gemäß § 44b SGB II zuständig.

#### **1. Jobcenter App allgemein**

Indem die App ausschließlich in den App-Stores der Betriebssystemhersteller Apple und Google angeboten wurde, waren die Nutzer gezwungen, deren Nutzungsbedingungen zu akzeptieren, wenn sie App nutzen wollten. Dies beinhaltete, dass personenbezogene Daten durch die Betriebssystemhersteller verarbeitet wurden, die nicht erforderlich waren, um die App zu beziehen. Mindestens die ausschließliche Bereitstellung der Apps über die Apple/Google-Stores verstieß somit gegen Art. 25 Abs. 2 DSGVO.

Ich sehe das Jobcenter diesbezüglich gemäß Artikel 25 Abs. 2 DSGVO in der Pflicht, geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Für die App des Jobcenters war der Bezug über die App-Stores der Betriebssystemhersteller technisch nicht notwendig. Beim Betriebssystem Android gibt es Alternativen zum Google Play Store: Die App kann in freien Stores oder auch als Android-Package-Datei (APK-Datei) auf der eigenen Webseiten bereitgestellt werden.

Die Öffnung von Apples iOS durch den Digital Markets Act wird es zukünftig ermöglichen, Apps nicht ausschließlich durch den Apple App-Store zu beziehen. Ich empfehle daher, für neue Apps die Situation zu beobachten und Apps für iOS zu gegebener Zeit auch außerhalb des Apple App-Stores zur Verfügung zu stellen.

Sofern als Rechtsgrundlage für die Nutzung der App Art. 6 Abs. 1 lit. a) DSGVO herangezogen wurde, sind die rechtlichen Bestimmungen zur Wirksamkeit einer Einwilligung gemäß Art. 7 und 8 DSGVO zu berücksichtigen. Als Anbieter eines digitalen Dienstes unterliegt das Jobcenter auch den Anforderungen des § 25 Abs. 1 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG). Als Maßstab für die Einwilligung weise ich auf die Orientierungshilfe Digitale Dienste<sup>1</sup> der Konferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hin.

Danach wies der vorliegende Einwilligungsdialo Defizite im Rahmen der Transparenz auf. Es wurde ausschließlich mit einem Link auf die Datenschutzerklärung verwiesen, jedoch hätte die Informationspflicht bzgl. die Einwilligung direkt im Dialog mindestens folgende Elemente enthalten müssen, die für die Entscheidungsfindung wesentlich sind: die Identität des Verantwortlichen, den Zweck jedes Verarbeitungsvorgangs, für den die Einwilligung eingeholt wird, die (Art der) Daten, die erhoben und verwendet werden und das Bestehen eines Widerrufsrechts.

Abseits der Modalitäten für eine rechtmäßige Einwilligung weise ich darauf hin, dass Datenverarbeitungen auf Rechtsgrundlage von Art. 6 Abs. 1 lit. e) DSGVO keiner Einwilligung bedürfen. Bei den gesetzlichen Aufgaben des Jobcenters, die sich in den Basisdiensten der App widerspiegeln (beispielsweise die Übersendung von Unterlagen), bedarf es keiner Einwilligung.

Anbieter von digitalen Diensten müssen bei Datenschutzinformationen darauf achten, die Vorgänge klar zu differenzieren. Sofern im Rahmen des digitalen Dienstangebotes Prozesse stattfinden, die sowohl unter das TDDDG als auch unter die DSGVO fallen, ist über die beide Rechtsgrundlagen jeweils separat zu informieren (mehr dazu unter Punkt 4 – Betroffenenrechte).

Folglich ist der Einwilligungsdialo beim erstmaligen Öffnen einer App so zu gestalten, dass die Einwilligung in informierter Weise erfolgt. So ist auf die Identität des Verantwortlichen, den Zweck jedes Verarbeitungsvorgangs, für den die Einwilligung eingeholt wird, die Art der Daten, die erhoben und verwendet werden und das Bestehen eines Widerrufsrechts direkt im Dialog hinzuweisen.

---

<sup>1</sup> [https://www.datenschutzkonferenz-online.de/media/oh/OH\\_Digitale\\_Dienste.pdf](https://www.datenschutzkonferenz-online.de/media/oh/OH_Digitale_Dienste.pdf)

## 2. Funktionsweise

Gemäß Art. 30 DSGVO hat der Verantwortliche ein VVT zu führen. Darin sind die Angaben aus Art. 30 Abs. 1. lit. a-g. DSGVO aufzuführen.

Die Angaben der Zwecke der Verarbeitung der Smartphone-App waren nicht differenziert genug:

Das Jobcenter gab im VVT den Zweck mit "Betrieb einer Smartphone-App für die Plattformen iOS (Apple) und Android (Google). Bereitstellung aller Online-Services auf einem mobilen Endgerät" an. Die angegebenen Zwecke spiegelten nicht wieder, zu welchen Zwecken die personenbezogenen Daten tatsächlich konkret verarbeitet wurden.

Laut der Datenschutzerklärung der Jobcenter App wurden beim Veranstaltungskalender, News-Feed, Mietpreisprüfer, Anzeige externer Webinhalte des Jobcenters keine personenbezogenen Daten verarbeitet. Dabei berücksichtigte das Jobcenter jedoch nicht, dass bereits der Abruf von Informationen von Servern des Jobcenters zwangsläufig mit einer Datenerhebung verbunden war. Schließlich wurde zur Herstellung der benötigten Netzwerkverbindung eine IP-Adresse benötigt, welche ein Datum ist, mit welchem Personen identifiziert werden können.

Die Beschreibung der technisch-organisatorischen Maßnahmen gemäß Art. 32 DSGVO im VVT muss daher so konkret sein, dass ich als Aufsichtsbehörde und der/die behördliche Datenschutzbeauftragte die Geeignetheit der Maßnahmen für ein angemessenes Schutzniveau vorliegend überprüfen können; vgl. Art. 39 Abs. 1 lit. b) DSGVO. Die im vorliegenden Fall dokumentierten technisch-organisatorischen Maßnahmen waren allgemein und bezogen sich auf die Sicherheit beim Auftragsverarbeiter bzw. beim Rechenzentrumsbetreiber. Spezifische technisch-organisatorische Maßnahmen, die sich auf die konkrete Verarbeitung des Jobcenters bezogen, waren hier nicht ersichtlich. Auch eine Orientierung an Referenzmaßnahmenkatalogen (z.B. BSI-Standards oder Standarddatenschutzmodell) war nicht erkennbar.

Beim VVT sind daher die einzelnen Verarbeitungen nach ihren Zwecken (z.B. Terminbuchung, Kontaktformular, Übermittlung von Unterlagen) zu trennen. Die Zwecke Veranstaltungskalender, News-Feed, Mietpreisprüfer, Anzeige externer Webinhalte des Jobcenters sind in das VVT aufzunehmen. IP-Adressen sind personenbezogene Daten und daher auch im VVT aufzuführen. Die technischen und organisatorischen Maßnahmen sind im VVT spezifisch darzustellen.

Hinsichtlich der getroffenen technisch-organisatorischen Maßnahmen bei der Übermittlung von Sozialdaten von der App an das Jobcenter halte ich die getroffenen Maßnahmen grundsätzlich für ausreichend. Ausschlaggebend hierfür ist, dass eine Auftragsverarbeitung vorlag und der (Unter)Auftragsverarbeiter somit verpflichtet war, Garantien für eine rechtmäßige Datenverarbeitung gegenüber dem Jobcenter zu geben.



Jedoch gebe ich zu bedenken, dass die übermittelten Sozialdaten unverschlüsselt im Hoheitsbereich des Auftragsverarbeiters lagen und erst von dort als verschlüsselte (S/MIME) E-Mail an das Jobcenter Oberhausen Postfach versendet wurden. Damit bestand ein vermeidbares Risiko für die Vertraulichkeit der Sozialdaten.

Um Risiken für die Vertraulichkeit zu reduzieren, empfehle ich in künftigen Fällen die Verschlüsselung unmittelbar im Client (App/Webbrowser) und die Entschlüsselung erst in der alleinigen Hoheit des Jobcenters durchzuführen, und somit eine Ende-zu-Ende-Verschlüsselung zu gewährleisten. Aus hiesiger Sicht wäre das möglich, da sowohl für JavaScript (Website), als auch für Android und iOS entsprechende Bibliotheken existieren. Die Funktionalität könnte also nachgerüstet werden. Eine Verschlüsselung ausschließlich mit Empfänger-Zertifikat ist im S/MIME-Standard vorgesehen (festgelegt in RFC 8551 unter Punkt 3.3). Darüber hinaus sind die Vorgaben der technischen Richtlinie BSI TR-03116 umzusetzen, die ich als den aktuellen Stand der Technik gemäß Art. 32 DSGVO betrachte. Alternativ kann eine Ende-zu-Ende-Verschlüsselung auch mittels PGP (Pretty Good Privacy) erreicht werden. Ein Parallelbetrieb von PGP und S/MIME ist grundsätzlich möglich.

Personenbezogene Daten sind zu löschen, wenn eine weitere Verarbeitung nicht mehr erforderlich ist (Art. 17 DSGVO). Um die Löschung zu gewährleisten, sind verbindliche Regelungen zur Löschung im Rahmen der DSGVO unverzichtbar. Aus den mir zur Verfügung gestellten Unterlagen waren verbindliche Regelungen/Weisungen zur Löschung nicht ersichtlich.

Diese sind in einem verschriftlichten Löschkonzept bzw. einer Weisung zu regeln und beinhalten, wann und wie die von einer App übermittelten Sozialdaten vom Jobcenter gelöscht werden. Weiterhin ist zu regeln, wann und wie die Protokolldateien, die im Rahmen der Verwendung der App beim Auftragsverarbeiter anfallen, gelöscht werden.

Gemäß Art. 25 DSGVO ist der Verantwortliche verpflichtet, geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich sind, verarbeitet werden. Zwar wurde beim erstmaligen Start der App abgefragt, ob Push-Mitteilungen aktiviert werden sollen. Jedoch, dass dieser Dienst eine Verbindung zu Google / Apple aufbaute, war zu diesem Zeitpunkt für Nutzende nicht ersichtlich. Es lagen damit Verstöße gegen Art. 25 und Art. 13 DSGVO vor und die Datenschutzerklärung hätte entsprechend ergänzt werden müssen.

Ich empfehle zudem, dass beim ersten Start der App nicht pauschal die Berechtigung für Push-Benachrichtigungen abgefragt wird, sondern nur, wenn der Dienst vom Nutzer ausdrücklich erwünscht wird. Die datenschutzfreundlichste Option wäre eine Erbringung der Funktionalität ohne Google/Apple und ohne die Nutzung proprietärer Online-Dienste von Drittanbietern. Dies wäre mittels „Polling“ oder einem eigenen



Benachrichtigungssystem möglich. Gemäß § 25 TDDDG bedarf es jedoch einer Einwilligung der Nutzer für die Nutzung der Push-Nachrichten, da diese nicht zum Basisdienst gehören.

### 3. Datenschutzmanagement

Eine Datenschutzfolgenabschätzung gemäß Art. 35 DSGVO ist durchzuführen, wenn die Form der Verarbeitung aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Recht und Freiheiten natürlicher Personen zur Folge hat. Ob ein voraussichtlich hohes Risiko durch eine Verarbeitungstätigkeit mit Personenbezug besteht, ist vorher im Rahmen einer obligatorischen Schwellenwert-Analyse festzustellen.

Das Jobcenter hätte demnach prüfen müssen, ob die Verarbeitungstätigkeit, für welche das Risiko zu bestimmen ist, in der „Muss-Liste“<sup>2</sup> gemäß Art. 35 Abs. 4 DSGVO der Datenschutzaufsichtsbehörden enthalten ist. In der Liste ist die Verarbeitung von Sozialdaten explizit aufgeführt und demnach ist von einem hohen Risiko auszugehen. Zudem konnten mittels der App auch besondere Kategorien von personenbezogenen Daten gemäß Art. 9 DSGVO übermittelt werden, bei denen stets ein hohes Risiko anzunehmen ist. Das Jobcenter hätte vor dem Einsatz der App eine Datenschutzfolgenabschätzung vornehmen müssen.

Auftragsverarbeiter ist gemäß Art. 4 Nr. 8 DSGVO eine Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Verantwortlicher ist gemäß Art. 4 Nr. 7 DSGVO die Stelle, die allein oder gemeinsam mit anderen über die Mittel und Zwecke der Verarbeitung personenbezogener Daten entscheidet. Hierbei kommt es maßgeblich auf die Entscheidung über die Verarbeitungszwecke an, während die Entscheidung über die technisch-organisatorischen Fragen der Verarbeitung auch auf den Auftragsverarbeiter delegiert werden kann.

In der Jobcenter App hatte das Jobcenter über die Mittel und Zwecke der Verarbeitung der Sozialdaten entschieden. Der Auftragsverarbeiter ist für die Umsetzung der technisch-organisatorischen Maßnahmen verantwortlich. Für eine Auftragsverarbeitung ist es irrelevant, ob personenbezogene Daten ausschließlich verschlüsselt über Server laufen. Auch wenn die Daten verschlüsselt übertragen werden, handelt es sich hierbei um eine Verarbeitung Sozialdaten. Daher lag eindeutig eine Auftragsverarbeitung vor und es war seitens des Jobcenters – nicht nur vorsorglich - einen Auftragsverarbeitungsvertrag abzuschließen.

Gemäß § 80 Abs. 1 SGB X ist eine Auftragsverarbeitung nur zulässig, wenn vor Erteilung des Auftrages die Informationen gemäß § 80 Abs. 1 Nr. 1-4 SGB X bei der Rechts- und Fachaufsicht angezeigt werden. Dies soll der Rechts- oder Fachaufsicht ermöglichen, bei

---

<sup>2</sup> [https://www.datenschutzkonferenz-online.de/media/ah/20181017\\_ah\\_DSK\\_DSFA\\_Muss-Liste\\_Version\\_1.1\\_Deutsch.pdf](https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf)

Zweifeln an der Ausgestaltung oder der Rechtmäßigkeit der Auftragsverarbeitung jedenfalls vorläufig die Auftragserteilung untersagen zu können. Aus den Unterlagen des Jobcenters ging nicht hervor, ob eine solche Anzeige für die Auftragsverarbeitung mit [REDACTED] an das Bundesministerium für Arbeit und Soziales als Aufsichtsbehörde stattgefunden hat.

Die Gesamtverantwortung für die Datenverarbeitung und Nachweispflicht des Verantwortlichen gemäß Art. 5 Abs. 2 DSGVO umfasst auch die Verarbeitung durch den Auftragsverarbeiter. Hiervon kann sich der Verantwortliche nicht durch die Beauftragung eines Auftragsverarbeiters befreien. Gemäß Art. 28 Abs. 1 DSGVO arbeitet ein Verantwortlicher nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Daraus ergibt sich in Verbindung mit Art. 32 Abs. 1 lit. d) DSGVO die Pflicht des Jobcenters, die Auftragverarbeiter sowie die Unterauftragverarbeiter regelmäßig während des gesamten Zeitraums der Zusammenarbeit zu kontrollieren. Dabei ist ein Konzept erforderlich, in dessen Rahmen der Verantwortliche planen muss, wie, wie oft und welche Auftragsverarbeiter er zu kontrollieren beabsichtigt. Dieser Verpflichtung ist das Jobcenter nicht nachgekommen ist. Für etwaige künftige Fälle ist ein Konzept zur regelmäßigen Kontrolle der (Unter)auftragsverarbeiter zu erstellen.

#### 4. Betroffenenrechte

Gemäß Art. 13 DSGVO hat das Jobcenter eine Informationspflicht bei der Erhebung personenbezogener Daten. Dieser Pflicht kam das Jobcenter im Rahmen der App mit den Datenschutzhinweisen grundsätzlich nach.

Als Rechtsgrundlage für die Verarbeitung der Daten in der App gab das Jobcenter in Punkt 1.5 seiner Stellungnahme vom 19. Februar 2024 Art. 6 Abs. 1 lit. a DSGVO (Einwilligung) an. Im aktuellen VVT der App war als Rechtsgrundlage neben Einwilligung zusätzlich "berechtigtes Interesse" angegeben. Diese Angabe fand sich auch in den Datenschutzhinweisen zur Smartphone-App wieder. Hier wurde unter Punkt 13 als Rechtsgrundlagen 6 Abs. 1 lit. a DSGVO (Einwilligung), sowie 6 Abs. 1 lit. f) DSGVO (berechtigtes Interesse) genannt.

In den Datenschutzhinweisen auf der Website des Jobcenters wurden verschiedene Rechtsgrundlagen angegeben. Eine Speicherung von Logdaten erfolgte auf Grundlage von berechtigten Interessen im Sinne des Art. 6 lit. f) DSGVO.

Bei dem Jobcenter handelt es sich um eine Behörde. Die in der App bereitgestellten Dienstleistungen dienen der Behörde zur Erfüllung ihrer Aufgaben. Damit kann sich das Jobcenter für diese Verarbeitungen nicht auf ein berechtigtes Interesse gemäß Art. 6 Abs. 1 lit. f) DSGVO stützen (siehe Art. 6 Abs. 1 UAbs. 2 DSGVO). In Bezug auf die Einwilligung als Rechtsgrundlage ist ebenfalls unklar, auf welche Verarbeitung sich diese speziell bezog.

In den Datenschutzhinweisen zur Smartphone-App wurde Art. 6 Abs.1 S. 1 lit. a) DSGVO im Zusammenhang mit der Erteilung von App-Berechtigungen für den Zugriff auf Kamera, Dateisystem und Kalender genannt. Offenbar setzte das Jobcenter das Erteilen von App-Berechtigungen mit der datenschutzrechtlichen Einwilligung gleich. Es erscheint fragwürdig, inwieweit die Einwilligung hierfür eine Rechtsgrundlage für die weitere Verarbeitung der damit erhobenen Daten beim Jobcenter darstellt. Insbesondere im Bereich der Daseinsfürsorge ist die Freiwilligkeit von Einwilligungen als Rechtsgrundlage durch Behörden kritisch zu sehen (vgl. Erwägungsgrund 43 DSGVO). Es hätte daher näher erläutert werden müssen, weshalb das Jobcenter hier ausnahmsweise eine Einwilligung für zulässig erachtet hat.

Eine Differenzierung, für welche Verarbeitung welche Rechtsgrundlage herangezogen wird, erfolgte durch das Jobcenter nicht. Es war zudem nicht nachvollziehbar, warum das Jobcenter die Verarbeitung über die Website und die App auf unterschiedliche Rechtsgrundlagen stützte. Die Anforderungen des Art. 13 Abs. 1 lit. c) DSGVO sind demnach nicht beachtet worden.

Auch bei den Services des Veranstaltungskalenders, News-Feeds, Mietpreisprüfers, Anzeige externer Webinhalte des Jobcenters, bei denen das Jobcenter angab, dass keine personenbezogenen Daten verarbeitet wurden, findet eine Datenverarbeitung statt. Bereits der Abruf von Informationen von Servern des Jobcenters ist zwangsläufig mit einer Datenerhebung verbunden. Schließlich wurde zur Herstellung der benötigten Netzwerkverbindung eine IP-Adresse benötigt und verarbeitet, welche ein Datum ist, mit welchem Personen identifiziert werden können (Art. 4 Nr. 1 DSGVO). Auch diesbezüglich wurde die Anforderungen des Art. 13 Abs. 1 lit. c) DSGVO nicht beachtet. Für künftige Fälle muss die Datenschutzerklärung folgende Punkte enthalten:

- Die Rechtsgrundlage gemäß Art. 6 Abs. 1 lit. f) DSGVO ist für Behörden unzutreffend und daher zu streichen und durch zulässige Grundlagen gemäß Art. 6 Abs. 1 lit. a) und e) i.V.m. Art. 6 Abs. 2 DSGVO und den spezifischen Rechtsgrundlagen im deutschen Recht zu ersetzen.
- Es ist zu differenzieren, für welche Verarbeitung welche zulässige Rechtsgrundlage herangezogen wird.
- IP-Adressen sind als personenbezogene Daten aufzunehmen.
- Die Verarbeitungszwecke „Veranstaltungskalender“, „News-Feeds“, „Mietpreisprüfers“, „Anzeige externer Webinhalte des Jobcenters“ sind aufzunehmen, da personenbezogene Daten verarbeitet werden.
- Die Angaben müssen in dem VVT und der Datenschutzerklärung übereinstimmend sein.
- Die Erteilung von App-Berechtigungen aufgrund von Art. 6 Abs. 1 lit. a) DSGVO ist zu streichen.

#### **4. Hinweis zur Veröffentlichung**

Erlauben Sie mir abschließend noch den folgenden Hinweis:

Die BfDI strebt ein modernes Informationsmanagement zwischen Bürger und Staat an, das eine Begegnung auf Augenhöhe ermöglichen soll. In Verfolgung dieses Ziels werden Kontrollberichte und/oder die jeweiligen Bescheide im rechtlich zulässigen Rahmen veröffentlicht. Sofern die kontrollierte Stelle dies wünscht, wird auch deren Stellungnahme veröffentlicht. Sofern der Kontrollbericht und/oder der darauf eventuell folgende Bescheid Namen einzelner natürlicher Personen enthalten, werden diese vor Veröffentlichung geschwärzt. Die Veröffentlichung erfolgt mit Bestandskraft des Bescheids bzw. in Fällen ohne Bescheid ca. einen Monat nach Übersendung des Kontrollberichts.

Mit freundlichen Grüßen

Im Auftrag

