Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

POSTANSCHRIFT Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Postfach 1468, 53004 Bonn

Bundesagentur für Arbeit
Regensburger Str. 104
90478 Nürnberg

nachrichtlich:

Herrn Wolfgang Nörenberg
Behördlicher Datenschutzbeauftragter
der Bundesagentur für Arbeit
- persönlich -
Regensburger Str. 104
90478 Nürnberg

HAUSANSCHRIFT Husarenstraße 30, 53117 Bonn
VERBINDUNGSBÜRO Friedrichstraße 50, 10117 Berlin

TELEFON (0228) 997799-213
TELEFAX (0228) 997799-550
E-MAIL referat12@bfdi.bund.de
BEARBEITET VON Silke Schäfer
INTERNET www.datenschutz.bund.de

DATUM Bonn, 12.01.2017
GESCHÄFTSZ. **12-302-1/038#0040**

Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

BETREFF **Datenschutzrechtlicher Beratungs- und Kontrollbesuch in der Zentrale der Bundesagentur für Arbeit**
HIER APOLLO (Antragsportal Leistungen Online)
BEZUG Mein Ankündigungsschreiben vom 25. Juli 2016

Sehr geehrte Damen und Herren,

vom 7. bis 9. September 2016 haben meine Mitarbeiter Herr Ernestus und Frau Schäfer einen Beratungs- und Kontrollbesuch nach § 81 Absatz 2 Satz 1 Zehntes Buch Sozialgesetzbuch (SGB X) i.V.m. §§ 24 bis 26 Bundesdatenschutzgesetz (BDSG) bei der Bundesagentur für Arbeit (BA) durchgeführt.

Der Besuch wurde von [redacted] in Vertretung des behördlichen Datenschutzbeauftragten der BA begleitet.
Für die gewährte konstruktive Unterstützung danke ich.

Gegenstand meines Beratungs- und Kontrollbesuchs war die Erhebung, Verarbeitung und Nutzung von Daten durch das IT-Verfahren APOLLO (Antragsportal Leistungen Online) und seine Schnittstellen. APOLLO stellt als Online-Portal Online-Antragsprozesse für Leistungen im SGB III sowie diverse Online-Prozessdienste

ZUSTELL- UND LIEFERANSCHRIFT Husarenstraße 30, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61, Husarenstraße

(z.B. Veränderungsmitteilungen) und Portalbasisdienste (z.B. eine Dokumentenablage) zur Verfügung. Zukünftig sollen zunehmend Leistungen der BA über das Portal online abgewickelt werden können.

Der Besuch hat zu folgenden Ergebnissen geführt:

- Die grundsätzliche IT-Sicherheitsarchitektur des Verfahrens ist bis auf offene Fragen zur Authentifizierung/Integrität datenschutzrechtlich angemessen.

- Die Authentifizierung der Personen, die APOLLO nutzen, muss, wie während des Beratungs- und Kontrollbesuchs vorgestellt, zeitnah angepasst werden. Im Hinblick auf den angestrebten Ausbau der Online-Verfahren sollten die geforderten Sicherheitsstufen für die eServices dringend überprüft werden.

- Die Integrität der über APOLLO in die eAkte eingestellten Dokumente ist zurzeit nicht ausreichend sicher gestellt. Hier besteht Handlungsbedarf.

- In den Portalen der BA muss klar zwischen den Bereichen getrennt werden, die reine Information seitens der BA enthalten und den Bereichen, die der Aufgabenerfüllung der BA nach dem Sozialgesetzbuch dienen. Dies bezieht sich nicht nur auf die unterschiedliche Behandlung der Stammdaten sogenannter Internetpersonen und Personen, die Kunden der BA sind, im Stammdatenerfassungs- und -pflegesystem der BA (STEP) und die Nutzungsbedingungen / Datenschutzerklärungen, sondern auch auf die Ausgestaltung der Portale. Hier wird vor allem im Anwenderportal Onlinekanal (APOK) Nachholbedarf gesehen.

Meine Feststellungen beruhen auf folgenden Erwägungen:

1. IT-Sicherheit allgemein

Die grundsätzliche IT-Sicherheitsarchitektur des Verfahrens APOLLO ist angemessen.
Dokumente, die die IT-Sicherheit gefährden, werden ausreichend blockiert. Dies entspricht den Anforderungen des BSI.
Allerdings ist die Fehlermeldung „Fehler 406" missverständlich. Sie wird angezeigt, wenn virenverseuchte Dokumente nicht hochgeladen werden können. Für den APOLLO-Nutzer ist aber weder erkennbar, dass er virenverseuchte Dokumente hoch

zu laden versucht noch ist die Fehlermeldung als solche verständlich. Hier sollte ein allgemeiner Hinweis auf IT-Sicherheitsprobleme für den Nutzer erfolgen, damit dieser beim unbewussten Versuch, schädliche Dokumente hoch zu laden, Maßnahmen gegen die bisher noch unbekannten IT-Sicherheitsprobleme auf seinem Rechner ergreifen und künftig APOLLO uneingeschränkt nutzen kann.

Ich bitte Sie, mir die geänderte Formulierung der Fehlermeldung zur Kenntnis zu geben.

2. Authentifizierung/Integrität

2.1 Authentifizierung Nutzer

APOLLO steht grundsätzlich jedem Internet-Nutzer offen und kann auch von „Nicht-Kunden" der BA besucht werden. Um die „eServices" (z.B. Arbeitsuchend melden, Arbeitslosengeld beantragen) nutzen zu können, bedarf es einer Registrierung.

APOLLO bedient sich dabei des Elektronischen Kunden- und Partneridentitätsmanagements der BA (EKIM). EKIM ist als Single Sign On konzipiert, d. h., das IT-Verfahren ist die Eingangstür zu jeglicher Nutzung der Online-Angebote der BA, wenn sich der Nutzer registriert. Dabei kann dieser zwischen fünf Sicherheitsstufen wählen:
Stufe 0: keine Überprüfung,
Stufe 1: E-Mail Bestätigung,
Stufe 2: PIN-Brief,
Stufe 3: Identifizierung durch Nutzung der eID-Funktion des Neuen Personalausweises (nPA) bzw. des elektronischen Aufenthaltstitels (eAT),
Stufe 4: Sichtprüfung der Ausweispapiere bei persönlicher Vorsprache in der Arbeitsagentur.
Der Nutzer kann die Sicherheitsstufe nach Abschluss der Registrierung erhöhen.

Die allgemeine Nutzung von APOLLO (Personalisierung, Dokumentenablage, Portalhistorienservice) und die Beantragung von Arbeitslosengeld sowie Berufsausbildungsbeihilfe durch Personen sind zurzeit ab Sicherheitsstufe 0 möglich. Bevor das Arbeitslosengeld ausgezahlt wird, erfolgt zwingend eine Vorsprache in der Arbeitsagentur. Die Berufsausbildungsbeihilfe wird nach Vorlage weiterer Unterlagen, wie z.B. dem Ausbildungsvertrag, dagegen ohne persönliche Vorsprache gewährt. Für Veränderungsmitteilungen über das Portal muss zumindest die Sicherheitsstu-

fe 2 ausgewählt worden sein. Für die Mitteilung von veränderten Kontodaten wird darüber hinaus eine Bestätigung durch mTAN verlangt. Betriebe benötigen für alle Anwendungen von APOLLO mindestens die Sicherheitsstufe 2, können bisher allerdings keine Leistungen über APOLLO beantragen.

Die Authentifizierung der Online-Portal-Nutzer ist die zentrale Grundlage für den datenschutzkonformen Betrieb eines solchen Portals. Hier hat die BA angemessene technische und organisatorische Maßnahmen zu treffen, um eine datenschutzkonforme Datenverarbeitung zu gewährleisten. Zu diesen technischen und organisatorischen Maßnahmen zählen u. a. die Zugriffs-, Weitergabe- und Eingabekontrolle. Deshalb muss sichergestellt sein, dass nur und ausschließlich der Nutzer Zugang zu seinen Daten erhält. Verschafft sich ein unbefugter Dritter Zugang zu diesen Daten, verstößt dies gegen § 12 Absatz 1 Telemediengesetz (TMG) i. V. m. § 14 Absatz 1 TMG bzw. § 67d Absatz 1 Zehntes Buch Sozialgesetzbuch (SGB X), da es an einer die Übermittlung an Dritte erlaubenden Rechtsnorm fehlt. Auch müssen die Daten der richtigen Person zugeordnet werden, damit innerhalb der BA nur die gemäß § 12 Absatz 1 TMG bzw. § 35 Absatz 1 Satz 2 Erstes Buch Sozialgesetzbuch (SGB I) berechtigten Personen Zugriff auf die Daten erhalten.

Während des Besuchs wurde meinen Mitarbeitern ein modifiziertes Authentifizierungsverfahren vorgestellt. Dieses sieht nunmehr für die Nutzung der eServices *Beantragung von Arbeitslosengeld / Berufsausbildungsbeihilfe* sowie *Veränderungsmitteilungen / Meldungen*, ergänzend zur Registrierung über EKIM, eine vorherige Vorsprache bei einer Agentur für Arbeit bzw. eine telefonische Authentifizierung in einem Service Center der BA vor. Dieser gestufte Authentifizierungsprozess soll mit der nächsten Programmversion auch auf *Insolvenzgeld online beantragen* erweitert werden. Ich halte dieses nunmehr modifizierte Authentifizierungsverfahren– entgegen der bisher vorgesehenen Authentifizierung – für grundsätzlich geeignet, die Authentizität der Nutzer von APOLLO sicher zu stellen. Unklar ist in diesem Zusammenhang jedoch, wie Sie die telefonische Authentifizierung datenschutzkonform gestalten wollen. Ich wäre Ihnen dankbar, wenn Sie mir das telefonische Authentifizierungsverfahren im Hinblick auf die datenschutzrechtlichen Anforderungen näher darlegen und mir den Umsetzungsstand des modifizierten Authentifizierungsverfahrens mitteilen könnten.

Für Ihr Ziel, die Abwicklung von Anträgen im Leistungsbereich SGB III in Zukunft als reinen Online-Prozess auszugestalten, rege ich bereits heute an, die Authentifizierung der Nutzer in EKIM von vornherein nur mit einer höheren Sicherheitsstufe vorzusehen.

2.2 Integrität Dokumente

Ist der Nutzer mit der entsprechenden Sicherheitsstufe registriert, kann er online seine Anträge ausfüllen, speichern und bearbeiten, die notwendigen Anlagen in die Dokumentenablage von APOLLO hochladen und alles an die BA übertragen. Die Antragsformulare und die hochgeladenen Dokumente werden dabei über eine Schnittstelle direkt als pdfA-Dokument in der elektronischen Akte der BA (eAkte) abgelegt. Diese Dokumente sind weder unterschrieben noch elektronisch signiert. Der Vorgang wurde vor Ort in Nürnberg bei der Agentur für Arbeit verifiziert.

§ 36a Absatz 1 SGB I sieht für alle Sozialleistungsbereiche des Sozialgesetzbuches vor, dass die Übermittlung elektronischer Dokumente zulässig ist, soweit der Empfänger hierfür einen Zugang eröffnet. An die Form der elektronischen Dokumente werden dabei keine besonderen Anforderungen gestellt. § 36a Absatz 2 SGB I legt lediglich für Dokumente, für die eine Rechtsvorschrift Schriftform anordnet, weitere Voraussetzungen für die der Schriftform gleichzustellende elektronische Form fest. Die in APOLLO bisher möglichen eServices bedürfen nach den jeweiligen Spezialvorschriften des SGB III keiner Schriftform. Die Antragstellung erfolgt vielmehr gemäß § 16 Absatz 1 Satz 1 SGB I formlos.

Neben der Feststellung, dass der Nutzer die Person ist, auf die sich die im Portal angegebenen Daten beziehen, muss im Online-Portal aber auch sichergestellt werden, dass Daten, die über das Portal in Anträgen oder Dokumenten übermittelt werden, mit den eingegebenen Daten übereinstimmen. Manipulationen durch Dritte sind auszuschließen, da diese einen Verstoß gegen § 12 Absatz 1 TMG i. V. m. § 14 Absatz 1 TMG bzw. § 67d Absatz 1 SGB X darstellen würden. Auch hier fehlt es insoweit an einer Rechtsnorm, die die Übermittlung der vom Nutzer eingetragenen, personenbezogenen Daten an Dritte erlaubt.

Der bisher vorgesehene, rein durch die technische Ausgestaltung der Übermittlung über eine Schnittstelle ausgestaltete Schutz vor Manipulation reicht aus hiesiger Sicht nicht aus, um die Integrität der vom Nutzer an die BA übermittelten Dokumente zu gewährleisten. Zumindest für eine Übergangszeit bitte ich Sie daher zu prüfen, ob ein Verfahren ähnlich dem in der Steuerverwaltung praktizierten ELSTER Verfahren Anwendung finden könnte. Durch die Bereitstellung von individuellen Zertifikaten zur Verschlüsselung und Unterschrift, die mit einer PIN für den Kunden abrufbar und

nutzbar wären, würde der Schutz vor Manipulation zumindest deutlich erhöht. Bitte teilen Sie mir das Ergebnis Ihrer Prüfung zeitnah mit.

Für Ihr Ziel, die Abwicklung von Anträgen im Leistungsbereich SGB III in Zukunft als reinen Online-Prozess auszugestalten, rate ich Ihnen zudem, entsprechend § 36a Absatz 2 SGB I qualifizierte elektronische Signaturen und De-Mail in APOLLO zu integrieren.

3. Unterschiedliche Behandlung Internetperson/Kunde

In den Portalen der BA wird nicht hinreichend klar zwischen der reinen Informationsbereitstellung und der Aufgabenerfüllung differenziert. Eine solche Bereichsdifferenzierung ist jedoch geboten, da sich die Datenerhebung, -verarbeitung und -nutzung insoweit auf unterschiedliche Rechtsgrundlagen stützen.

Personen, die sich lediglich als Nutzer registrieren, um sich die Informationsangebote der BA z.B. mit Merklisten zu strukturieren, zählen zu den sog. Internetpersonen und unterfallen den Regelungen des Telemediengesetzes. Ihre personenbezogenen Daten stellen keine Sozialdaten i. S. d. § 67 Absatz 1 SGB X dar, da der Bezug auf eine aktuelle Aufgabe der BA nach dem Sozialgesetzbuch fehlt. Vielmehr sind diese Daten als Bestandsdaten nach § 14 Absatz 1 TMG zu bewerten, die nur zum Zweck der Nutzerbetreuung gespeichert und verwendet werden dürfen.

Die personenbezogenen Daten von Kunden der BA, die Leistungen der BA in Anspruch nehmen und z. B. ihre Anträge online übermitteln, sind hingegen Sozialdaten i. S. d. § 67 Absatz 1 SGB X. Für sie gilt das Sozialgeheimnis nach § 35 Absatz 1 Satz 1 SGB I und die BA darf diese personenbezogenen Daten nach den Vorschriften des SGB III und des SGB X für ihre Aufgabenerfüllung nutzen.

3.1 Behandlung in STEP

Die Stammdaten der Internetpersonen und der BA-Kunden werden logisch getrennt in der STEP-Datenbank gespeichert. Zum Zeitpunkt des Kontrollbesuchs war der Zugriff auf die Stammdaten technischerseits allerdings noch nicht auf die mit der Nutzerbetreuung betrauten Mitarbeiter der BA beschränkt, sondern nur durch organisatorische Maßnahmen eingegrenzt. Sie haben zugesagt, zur Programmversion P63, die am 21. November 2016 live geschaltet werden sollte, eine entsprechende Zugriffsbeschränkung einzurichten.

Wie bereits mehrfach erläutert, müssen aufgrund der unterschiedlichen Rechtsgrundlagen auch die Stammdaten der Internetpersonen und der BA-Kunden getrennt gespeichert und der Zugriff auf die Bestandsdaten nach dem Telemediengesetz beschränkt werden. Leider haben Sie zunächst von einer wirksamen Zugriffsbeschränkung abgesehen. Dies stellt einen gravierenden Verstoß gegen das Trennungsgebot in der Anlage zu § 9 BDSG dar. Da Sie allerdings meinen Mitarbeitern im Rahmen des Beratungs- und Kontrollbesuchs glaubhaft versichert haben, diesen Verstoß mit der Programmversion P63 zu beheben, sehe ich gemäß § 25 Absatz 2 BDSG von einer Beanstandung ab.

Stellt ein Internetkunde einen Leistungsantrag bei der BA und willigt dabei in die Verarbeitung und Nutzung seiner als Internetperson angegebenen Daten gemäß § 67c Absatz 2 Nummer 2 SGB X ein, werden seine bis dahin als Internetkunde gespeicherten Daten in den BA-Kundenbereich der STEP-Datenbank überführt. Leider konnte während der Kontrolle nicht geklärt werden, welche Daten übernommen werden. Ich wäre deshalb für eine Mitteilung dankbar, welche Daten der Internetperson letztendlich übernommen werden und zu welchen Zwecken.

Zudem gehe ich davon aus, dass Zugriffe der Mitarbeiter der BA auf die Stammdaten von BA-Kunden inzwischen, wie von Ihnen im Rahmen der Kontrolle von STEP zugesichert, 90 Tage protokolliert werden. Auch Zugriffe der Mitarbeiter der BA auf die Stammdaten von Internetpersonen sollten 90 Tage protokolliert werden.

Ich bitte insoweit um Stellungnahme zur aktuellen Protokollierung in STEP. Darüber hinaus bitte ich, mir zu bestätigen, dass die Programmversion P63 tatsächlich ab dem 21. November 2016 eine getrennte Speicherung vorsieht.

3.2 Behandlung in APOLLO

In APOLLO erfolgt eine Nutzerinformation. Dieser wird darauf hingewiesen, dass er sich in den Bereich der gesetzlichen Aufgabenerfüllung der BA mit den weitergehenden Rechten zur Datenerhebung, -verarbeitung und –nutzung nach den SGB III und X begibt. Dieser Hinweis findet sich am Ende eines jeden Antrags, der als eService gestellt werden kann. Allerdings entspricht der bisher verwandte Text nicht den Anforderungen an eine Einwilligung nach § 67c Absatz 2 Nummer 2 SGB X. Bitte übermitteln Sie mir hierzu einen neuen Textvorschlag.

Das Berechtigungs- und Rollenkonzept zu APOLLO sieht vor, dass Internetkunden Veränderungsmitteilungen an die BA übermitteln können. Veränderungsmitteilungen können aber anderseits nur von Personen übermittelt werden, die bereits Kunde der BA sind. Ich möchte Sie daher bitten, das Berechtigungs- und Rollenkonzept und die entsprechend vorgesehene technische Berechtigung im Portal konsistent abzuändern und mich über die Änderung zu unterrichten.

3.3 Behandlung in APOK

Im Rahmen der geplanten Weiterentwicklung des Internetangebots der BA wird den bisher schon auf der Internetseite der BA vorhanden Informationen ab Dezember 2016 schrittweise ein Anwenderportal Onlinekanal (APOK) vorgeschaltet, das die Navigation vereinfacht, Angebote bündelt und ab 2017 die Portalfunktionen von APOLLO integriert. Dabei werden die Nutzer wie bisher in drei Gruppen unterteilt: Privatpersonen, Unternehmen und Institutionen. Jede Gruppe wird dann mit unterschiedlichen Lebensbereichskacheln zu den sie interessierenden Angeboten gelenkt. Dabei ist nicht ersichtlich, welche Bereiche reine Information durch die BA darstellen und welche Bereiche der Aufgabenerfüllung der BA nach dem Sozialgesetzbuch dienen.

Dem Nutzer des Internetangebots der BA muss aber eindeutig und transparent klar werden, wo er frei über seine Daten verfügt und ab wann diese aufgrund der gesetzlichen Grundlage im SGB III und X von der BA erhoben, verarbeitet und genutzt werden dürfen. Hier sollte das Design von APOK, z.B. mit einer farblichen Unterscheidung, angepasst werden.

3.4 Nutzungsbedingungen/Datenschutzerklärung

Zurzeit gibt es für jede Online-Anwendung der BA eigene Nutzungsbedingungen und Datenschutzerklärungen. Die Nutzer von APOLLO müssen die Datenschutzerklärung der BA-Internetseite zur Kenntnis nehmen, bei der Registrierung die Nutzungsbedingungen von EKIM akzeptieren und die entsprechende Datenschutzerklärung konsultieren und abschließend die Nutzungsbedingungen von APOLLO akzeptieren und sich mit der entsprechenden Datenschutzerklärung informieren. Während des Kontrollbesuchs haben Sie meinen Mitarbeitern mitgeteilt, Sie überarbeiteten zurzeit die Nutzungsbedingungen und die Datenschutzerklärungen im Online-Portal der BA. Ziel sei dabei, einheitliche übergreifende Nutzungsbedingungen und eine Datenschutzerklärung für das gesamte Online-Portal der BA zu formulieren. Dies begrüße ich sehr. Meine Mitarbeiter haben aufgrund des bereits angestoßenen Überarbeitungsprozesses von einer inhaltlichen Prüfung der bisherigen Nutzungsbedingungen und der Datenschutzerklärung abgesehen. Daher möchte ich Sie bitten, zeitnah den neuen Entwurf zur Abstimmung vorzulegen.

4. Weitere Empfehlungen

Bei der Registrierung über EKIM muss der Nutzer ein E-Mail-Postfach angeben. An dieses Postfach wird ein Bestätigungslink zur Registrierung gesendet. Ohne Bestätigung des Links kann der Account nicht genutzt werden. Leider kann eine falsche E-Mail-Adresse nicht mehr korrigiert werden, d. h., die Bestätigungsmail kann nicht aufgerufen und die Registrierung nicht abgeschlossen werden. Warum eine Korrektur der E-Mail-Adresse nicht möglich sein sollte, konnte leider nicht abschließend geklärt werden. Daher muss die Registrierung derzeit in Fällen etwa eines Rechtschreibfehlers wiederholt werden, wodurch es zwangsläufig zu Dubletten im Internet-Nutzerbereich kommt. Ich rege an, die Korrektur falscher Angaben bei der ersten Registrierung oder einen „kontrollierten" Abbruch zu ermöglichen, um den Registrierungsprozess zuverlässig beenden zu können.

Die Administration des APOLLO-Verfahrens erfolgt derzeit auch unter Zuhilfenahme externer Mitarbeiter. Es handelt sich hierbei um Datenverarbeitung im Auftrag. Die besonderen Formvorschriften des § 11 BDSG/des § 80 SGB X sind dabei zu beachten. Aufgrund der schützenswerten Daten, die im Verfahren APOLLO verarbeitet werden, bitte ich um Bestätigung, dass alle Regelungen des § 11 BDSG/des

§ 80 SGB X eingehalten werden und alle externen Mitarbeiter nach § 5 BDSG (Datengeheimnis) verpflichtet wurden. Die Mitwirkung von externen Mitarbeitern ist aufgrund der Sensibilität der verarbeiteten Daten auf ein Minimum zu beschränken.

Für eine Stellungnahme innerhalb von 12 Wochen wäre ich dankbar.

Mit freundlichen Grüßen
In Vertretung

Gerhold