Geschäftsanweisung

Nr. 1 / 2021

Geschäftszeichen: **II-2081**

Gültigkeit ab: **11.03.2021**
Gültigkeit bis: **unbegrenzt**

Verteiler: **alle Mitarbeiter*innen**

letzte Aktualisierung: 29.09.2021

jobcenter Berlin Neukölln

Geschäftsanweisung zur Meldepflicht bei Verletzungen des Schutzes personenbezogener Daten

Festlegungen der Berichtswege und der Entscheidungszuständigkeiten bei Verletzungen des Schutzes personenbezogener Daten (Art. 33 DSGVO i.V.m. § 83a SGB X)

Inhaltsverzeichnis

1. Ausgangssituation
2. Ziel
3. Grundlagen
    - 3.1 Verantwortliche
    - 3.2 Verletzung des Schutzes personenbezogener Daten
    - 3.3 Meldepflicht und Meldefrist
    - 3.4 Rechte und Freiheiten natürlicher Personen und Risikobewertung
4. Meldeverfahren im JC
    - 4.1 Information durch das Servicecenter
    - 4.2 Hausinterne Informationsweiterleitung
    - 4.3 Bearbeitung im zuständigen Team
    - 4.4 Risikobewertung und Meldung der Verletzung des Schutzes personenbezogener Daten
    - 4.5 Dokumentation im JC
5. Datenschutz und IT-Sicherheit
6. Schulung
7. Schlussbestimmungen /Inkrafttreten

1. Ausgangssituation

Ausgangs-situation

Seit dem 25.05.2018 gilt die Europäische Datenschutz-Grundverordnung (DSGVO) als verbindliche gesetzliche Regelung zum Schutz der personenbezogenen Daten in allen EU-Mitgliedsstaaten. Mit dem Datenschutz-Anpassungs- und Umsetzungsgesetz EU vom 30.06.2017 und dem Zweiten Datenschutz-Anpassungs- und Umsetzungsgesetz EU - 2. DSAnpUG vom 26.11.2019 wurden die datenschutzrechtlichen Regelungen unter anderem der Sozialgesetzbücher (SGB) und des Bundesdatenschutzgesetzes (BDSG) an die DSGVO angepasst.

Damit müssen seit dem 25.05.2018 alle Verletzungen des Schutzes personenbezogener Daten an die/den Bundesbeauftragte/n für den Datenschutz und die Informationsfreiheit (BfDI) und an das Bundesministerium für Arbeit und Soziales (BMAS) gemeldet werden, wenn voraussichtlich ein Risiko für die Rechte und Freiheiten der betroffenen Personen besteht.

2. Ziel

Erfüllung der gesetzlichen Anforderungen

Um die gesetzlichen Anforderungen, insbesondere die Prüfung der Meldepflicht und die Einhaltung der Meldefrist von 72 Stunden sicherzustellen, werden mit dieser Weisung die Berichtswege und die Entscheidungszuständigkeiten bei Verletzungen des Schutzes personenbezogener Daten im Jobcenter Berlin Neukölln (JC) festgelegt.

3. Grundlagen
3.1 Verantwortliche

Verantwortliche

Die/Der Verantwortliche ist verpflichtet, Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörden - BfDI und BMAS - zu melden (Art. 33 DSGVO und § 83a SGB X).

Verantwortliche/r ist der Vorstand bzw. die jeweilige Geschäftsführung der Behörde, die über die Zwecke und Mittel der Datenverarbeitung entscheidet (Art. 4 Nr. 7 DSGVO).

Für den Rechtskreis SGB III ist das grundsätzlich der Vorstand der Bundesagentur für Arbeit und **für den Rechtskreis SGB II ist dies grundsätzlich die jeweilige Geschäftsführung einer gE** bzw. eines JC mit nachfolgender Ausnahme.

Grundsätzlich ist die gemeinsame Einrichtung Verantwortliche (§ 50 Abs. 2 SGB II). Für die zentral verwalteten Verfahren der Informationstechnik ist die Bundesagentur für Arbeit (BA) Verantwortliche im Sinne der DSGVO (§ 50 Abs. 3 S. 2 SGB II). Das Gleiche gilt für Dienstleistungen, die nach § 44b Abs. 5 SGB II vom JC eingekauft und Aufgaben, die gemäß § 44b Abs. 4 SGB II auf die BA (rück-)übertragen wurden.

Verletzungen des Schutzes personenbezogener Daten, die bei einer auftragsverarbeitenden Stelle bekannt werden, müssen durch die verantwortliche Stelle, also das JC, gegenüber den Aufsichtsbehörden gemeldet werden (Art. 33 Abs. 2 DSGVO). Auftragsverarbeitende sind Stellen, die Daten im Auftrag des JC verarbeiten (z.B. Dolmetschende, Scandienstleistende, Firmen der Aktenvernichtung). Die Eigenschaft als Auftragsverarbeitende ergibt sich aus dem jeweiligen zugrundeliegenden Vertrag. Bei Bildungsträgern, Maßnahmenträgern und Auftragnehmern, deren Vertragsgegenstand nicht die Verarbeitung von personenbezogenen Daten ist (z.B. Reinigungsdienstleistende), handelt es sich nicht um Auftragsverarbeitende. Diese Stellen müssen eventuelle Datenschutzverletzungen in eigener Zuständigkeit bearbeiten und melden.

3.2 Verletzungen des Schutzes personenbezogener Daten

Verletzungen des Schutzes personen-bezogener Daten

Eine Verletzung des Schutzes personenbezogener Daten ist eine Verletzung der Sicherheit, die, ob unbeabsichtigt und unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden (Art. 4 Nr. 12 DSGVO).

Verletzungen des Schutzes personenbezogener Daten sind z.B.:

- die unberechtigte Kenntnisnahme von personenbezogenen Daten, beispielsweise bei Versand an eine/n falsche/n Empfänger/in oder bei Bekanntgabe von personenbezogenen Daten gegenüber unberechtigten Dritten;
- der Verlust von personenbezogenen Daten z.B. bei Diebstahl oder Verlust von MAP's, mobilen Datenträgern und Dokumenten (z.B. Akten oder Ausdrucken aus Fachverfahren);
- die Manipulationen von personenbezogenen Daten, z.B. eigenmächtige Änderungen der Stammdaten, der Bankverbindung;
- die Meldung einer auftragsverarbeitenden Person über eine Verletzung des Schutzes personenbezogener Daten.

3.3 Meldepflicht und Meldefrist

Meldepflicht und Meldefrist

Verletzungen des Schutzes personenbezogener Daten sind gemäß Art. 33 Abs. 1 DSGVO i.V.m. § 83a SGB X innerhalb von 72 Stunden an die/den BfDI und das BMAS zu melden, wenn die Datenschutzverletzung voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

3.4 Rechte und Freiheiten natürlicher Personen und Risikobewertung

Rechte und Freiheiten natürlicher Personen

„Rechte und Freiheiten natürlicher Personen" ist als zentraler Begriff in der DSGVO und im europarechtlichen Kontext auszulegen. Dazu gehören

neben dem Grundrecht auf Schutz personenbezogener Daten aus Art. 8 der Charta der Grundrechte der Europäischen Union (GrCh) das Recht auf informationelle Selbstbestimmung und zudem einfachgesetzliche individuelle Rechte.

Risikobewertung

Der Begriff des Risikos ist in der DSGVO nicht ausdrücklich bestimmt. Zu verstehen ist darunter das Bestehen der Möglichkeit des Eintrittes eines Ereignisses, das selbst einen Schaden (einschließlich ungerechtfertigter Beeinträchtigungen von Rechten und Freiheiten natürlicher Personen) darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann[1].
Physische, materielle und immaterielle Schäden sind als mögliche Schäden einzuordnen (Erwägungsgrund 75 der DSGVO). Ungerechtfertigte Beeinträchtigungen von Rechten und Freiheiten natürlicher Personen (Grundrechtsverletzungen) sind den immateriellen Schäden zuzurechnen.

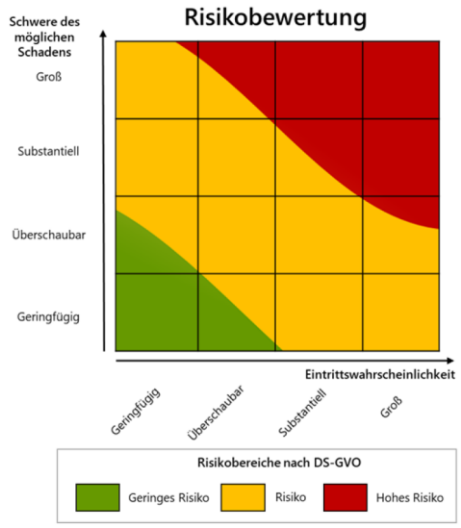
Für die Einschätzung des voraussichtlichen Risikos für die Rechte und Freiheiten von natürlichen Personen sind alle denkbaren negativen Folgen für natürliche Personen (wirtschaftliche, finanzielle und immaterielle Interessen, Zugang zu Gütern und Dienstleistungen, berufliches und gesellschaftliches Ansehen, gesundheitlicher Zustand und sonstige legitime Interessen) zu beachten. Mögliche Schäden können u.a. sein:

- Diskriminierung,
- Rufschädigung,
- Identitätsdiebstahl,
- finanzieller Verlust,
- wirtschaftliche oder gesellschaftliche Nachteile,
- Ausschluss oder Einschränkung der Ausübung von Rechten und Freiheiten.

Die Schwere des Schadens muss im jeweiligen Einzelfall unter Berücksichtigung von Art, Umfang und Zweck der Datenverarbeitung bestimmt werden. Beurteilungskriterien sind beispielsweise:

- die Verarbeitung betrifft besondere Kategorien personenbezogener Daten (Art. 9 DSGVO), für die ein ausdrücklich gesteigertes Schutzbedürfnis besteht;
- die Verarbeitung betrifft schützenswerte Personengruppen (z.B. Kinder);
- es handelt sich um Verarbeitungen, die eine systematische Überwachung ermöglichen;
- es werden Daten einer großen Anzahl von betroffenen Personen verarbeitet.

[1] Kurzpapier der Datenschutzkonferenz Nr. 18, S. 1



Zur Risikobewertung sind die Schwere des möglichen Schadens und die mögliche Eintrittswahrscheinlichkeit zu beurteilen.[2]

Alle Verletzungen des Schutzes personenbezogener Daten, die voraussichtlich zu einem Risiko für die Rechte und Freiheiten von natürlichen Personen führen, sind meldepflichtig.

Bei Verletzungen des Schutzes personenbezogener Daten, die Sozialdaten betreffen, ist aufgrund der besonderen Schutzbedürftigkeit, die sich allein aus dem Sozialgeheimnis ergibt, grundsätzlich von einem bestehenden Risiko auszugehen.

4. Meldeverfahren im JC

Meldeverfahren

Verantwortlich für die fristgerechte Beurteilung und Meldung von Verletzungen des Schutzes personenbezogener Daten ist die Geschäftsführung des JC. Durch die Festlegung des Berichtsweges und des Meldeverfahrens soll die Erfüllung der gesetzlichen Anforderungen sichergestellt werden. Das Ablaufschema kann aus der **Anlage F** zur Hilfestellung entnommen werden.

4.1 Information durch das Servicecenter

Information durch das Servicecenter

In vielen Fällen melden sich die Betroffenen oder die unberechtigten Empfänger/innen, denen personenbezogene Daten offenbart wurden, im Servicecenter. Durch das Servicecenter werden die Informationen zur unrechtmäßigen Datenoffenbarung gegenüber unberechtigten Dritten als Ticket **per verschlüsselter E-Mail** an folgendes Postfach übersandt:
Jobcenter-Berlin-Neukoelln.Datenschutzmeldung@jobcenter-ge.de

[2] Kurzpapier der Datenschutzkonferenz Nr. 18, S. 5 (Anlage A)

Durch die/den Mitarbeiter*in in Datenschutzangelegenheiten und den gesondert zu bestimmenden Mitarbeiter*innen des Teams 647 in unterstützender fachlicher Vertretung, erfolgt die **verschlüsselte Weiterleitung** des Tickets und des dazugehörigen internen Meldebogens (Anlage B) an die jeweils zuständige Teamleitung bzw. deren Vertretung (Leiste, MuI, SGG, usw.). Zusätzlich steht eine Ausfüllhilfe der BA hierfür als Anlage C zur Verfügung.

Die für dieses Team zuständige Bereichsleitung wird durch die Cc-Setzung ebenfalls informiert.

Zuständig ist jeweils das Team, in dem sich die Verletzung des Schutzes personenbezogener Daten ereignet hat, bzw. das Team, in dem die betroffene Person betreut wird (MuI und LG).

Die Weiterleitung an die zuständige Teamleitung muss unverzüglich (taggleich) erfolgen.

Darüber hinaus ist der Fall von der/dem Mitarbeiter*innen in Datenschutzangelegenheiten in die Datenbank Datenschutzmeldungen mit den erforderlichen Daten (von wem kommt die Meldung, Datum des Eingangs und Teamangabe bzgl. der Weiterleitung) einzutragen.

4.2 Hausinterne Informationsweiterleitung

Hausinterne Informations-weiterleitung

Wird eine Verletzung des Schutzes personenbezogener Daten im JC durch die/den Betroffene/n (Kundin bzw. Kunde), eine Mitarbeiterin bzw. einen Mitarbeiter oder einen anderen Dritten mitgeteilt bzw. bekannt gegeben, ist diese Information unverzüglich (taggleich) an die eigene Teamleitung weiterzuleiten.

Die zuständige Teamleitung bzw. deren Vertretung leitet diese Meldung zunächst an das nachfolgende E-Mail-Postfach **verschlüsselt weiter**:

Jobcenter-Berlin-Neukoelln.Datenschutzmeldung@jobcenter-ge.de

Sofern die zuständige Teamleitung nicht anwesend ist und auch nicht vertreten wird, hat die/der zuständige Mitarbeiter*in des Teams die entsprechende Meldung an das obige Postfach **verschlüsselt weiterzuleiten**. Die jeweils zuständige Fachbereichsleitung ist hierbei in Cc zu setzen.

Soweit die jeweils meldende Teamleitung bzw. deren Mitarbeiter*in nicht fachlich zuständig sind, ist der Vorgang für dieses Team abgeschlossen. Sofern sie fachlich für die Betreuung dieser Kundin /dieses Kunden zuständig ist (MuI/LG) bzw. sich der Datenschutzvorfall in diesem Team ereignet hat, erfolgt die weitere Bearbeitung des Falles (siehe hierzu unter 4.3).

Erfolgt die **verschlüsselte Meldung** eines fachlich nicht zuständigen Teams an das Organisationspostfach Datenschutzmeldung, ist die/der Mitarbeiter*in in Datenschutzangelegenheiten bzw. sind die gesondert zu bestimmenden Mitarbeiter*innen des Teams 647 in unterstützender fachlicher Vertretung für die **verschlüsselte Weiterleitung** an die jeweils zuständige/n Teamleitung/en (inkl. des internen Meldebogens) verantwortlich und setzen zusätzlich die jeweils zuständige/n Bereichsleitung/en in Cc.

Zuständig ist das Team, in dem sich die Verletzung des Schutzes personenbezogener Daten ereignet hat, bzw. das Team, in dem die betroffene Person betreut wird (MuI und auch LG).

4.3. Bearbeitung im zuständigen Team und Risikobewertung

Bearbeitung im zuständigen Team

Der zugrundeliegende Sachverhalt wird durch die zuständige Teamleitung oder deren Vertretung **innerhalb eines Arbeitstages geprüft und der ermittelte Sachverhalt in dem internen Meldebogen (Anlage B) für Datenschutzverletzungen erfasst**.

Sofern die zuständige Teamleitung nicht anwesend ist und auch nicht vertreten wird, ist **durch die jeweils zuständige Bereichsleitung sicherzustellen**, dass die erforderliche Rückmeldung inkl. des ausgefüllten Meldebogens spätestens an diesem Tag verschlüsselt an das Postfach _BA-Jobcenter-Berlin-Neukölln-Datenschutzmeldung erfolgt.

Bei fachlichen Fragen zum Datenschutz bei der Dokumentation innerhalb des Meldebogens kann die/der behördliche Datenschutzbeauftragte (bDSB) zur fachlichen Unterstützung hinzugezogen werden.

Anschließend wird der Meldebogen taggleich **per verschlüsselter E-Mail** an die zuständige Bereichsleitung oder deren fachliche Vertretung gesandt.

Handelt es sich bei der Verletzung des Schutzes personenbezogener Daten um eine vorsätzliche Datenschutzverletzung einer Mitarbeiterin/eines Mitarbeiters des JC, ist in der **verschlüsselten Meldung** an das nachfolgende E-Mail-Postfach gesondert darauf hinzuweisen:

Jobcenter-Berlin-Neukoelln.Datenschutzmeldung@jobcenter-ge.de.

Neben der Ermittlung des Sachverhalts durch die **zuständige Teamleitung** hat **durch die zuständige Bereichsleitung** eine (fachlich abschließende) Risikobewertung zu erfolgen (siehe hierzu oben unter 3.4).
Weiterhin ist durch die zuständige Bereichsleitung sicherzustellen, dass geeignete Maßnahmen nach einem Datenschutzfall ergriffen werden, welche neben der Sensibilisierung der betroffenen Mitarbeiter*in eine deutliche Verringerung solcher Datenschutzverletzungen gewährleisten bzw. Wiederholungen vermeiden. Diese Maßnahmen sind im Meldebogen durch die zuständige Team- bzw. Bereichsleitung zu dokumentieren und nachzuhalten. Sollte ein Datenschutzverstoß außerhalb der eigenen

Zuständigkeit erfolgt sein (z.B. Poststelle bzgl. einer Fehlkuvertierung), meldet die bearbeitende Bereichsleitung dies an die zuständige Bereichsleitung (aktuell BL67) weiter und empfiehlt hierzu geeignete Maßnahmen oder stimmt diese gemeinsam ab.

(abschließende) Risikobewertung

Sofern nach dieser Bewertung ein voraussichtlich **hohes Risiko** für die Rechte und Freiheiten der/des Betroffenen besteht, ist die **betroffene Person schriftlich per PZU über die eingetretene Verletzung zu informieren** (Art. 34 DSGVO).
Das Schreiben an die/den Betroffene/n ist in Kopie durch die zuständige Bereichsleitung per verschlüsselter E-Mail an Jobcenter-Berlin-Neukoelln.Datenschutzmeldung@jobcenter-ge.de zum Vorgang zu übersenden.

Bei Abwesenheit der zuständigen Bereichsleitung erfolgt diese Meldung durch die stellvertretende Bereichsleitung.

Ein hohes Risiko für die Rechte und Freiheiten der Betroffenen ist insbesondere dann anzunehmen, wenn die Verletzung des Schutzes besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO betrifft (z.B. Gesundheitsdaten), wenn besonders schützenswerte Personengruppen betroffen sind (Kunden mit S- und M-Kennzeichen, Kinder) oder wenn besonders schützenswerte Daten (z.B. Bankverbindungen) offenbart wurden.

Zur Hilfestellung bei der Bewertung wird auf den vorherigen Punkt 3.4 dieser GA verwiesen.

Bei einem darüberhinausgehenden Bedarf kann die/der bDSB zur fachlichen Unterstützung angefragt werden.

4.4 Meldung der Verletzung des Schutzes personenbezogener Daten

Die abschließende Bearbeitung und Weiterleitung an die zuständigen Stellen erfolgt durch die/den Mitarbeiter*in in Datenschutzangelegenheiten bzw. den gesondert zu bestimmenden Mitarbeiter*innen des Teams 647 in unterstützender fachlicher Vertretung.

Meldung an die Zuständige/n Stellen (Stabsstelle oder BMAS und BfDI)

Sofern die Verletzung des Schutzes personenbezogener Daten die zentral verwalteten Verfahren der Informationstechnik, eine eingekaufte Dienstleistung der BA oder eine an die BA übertragene Aufgabe betrifft, ist der vollständig ausgefüllte interne Meldebogen **an die Stabsstelle Datenschutz der BA per verschlüsselter E-Mail weiterzuleiten.**

Zusätzlich ist die Meldung in Cc an die jeweils betroffenen Bereichsleitungen zur Kenntnis zu senden.

Diese Übersendung **muss spätestens innerhalb 48 Stunden** nach Bekanntwerden der Verletzung des Schutzes personenbezogener Daten erfolgen.
Wird diese Frist überschritten, muss zwingend eine schriftliche Begründung für die Überschreitung dieser Frist innerhalb des Meldebogens erfolgen.

Sofern die Verletzung des Schutzes personenbezogenen **Daten in der Verantwortung des JC nach § 50 Abs. 2 SGB II liegt, ist die Meldung an die/den BfDI und das BMAS als anonymisierte Meldung (ohne Angabe von z.B. Kunden- oder BG-Nummer und Namen von Betroffenen oder Mitarbeiter*in)** mittels eines vereinfachten Meldebogen (Anlage D) zu senden.

Wichtig ist, hierbei zu beachten, dass das jeweilige Kreuz des richtigen Empfängers gesetzt wird.

Dieser vereinfachte Meldebogen ist dann per E-Mail **unverschlüsselt**

an den BfDI

und

das BMAS ,

zu übersenden.

Auch diese Meldung ist in Cc an die jeweils betroffenen Bereichsleitungen zur Kenntnis zu senden.

Diese Meldung **muss innerhalb von 72 Stunden nach Bekanntwerden** der Verletzung des Schutzes personenbezogener Daten erfolgen.

Wird diese Frist überschritten, muss zwingend eine schriftliche Begründung für die Überschreitung dieser Frist innerhalb des Meldebogens erfolgen.

Hinweis:
Begehen Mitarbeiter*innen vorsätzlich Datenschutzverstöße, schwingen sie sich damit zu einem eigenen Verantwortlichen im Sinne der DSGVO auf. Die Zuständigkeit für die Bearbeitung derartiger Verstöße liegt in diesen Fällen bei der/dem Berliner Landesbeauftragten für den Datenschutz und die Informationsfreiheit.
Die Meldung der Verletzung des Schutzes personenbezogener Daten **kann** in Absprache mit der Geschäftsführung neben der Meldung an das BMAS und die/den BfDI **zusätzlich auch an diese Behörde erfolgen**. Die/Der bDSB wird in einem solchen Datenschutzfall frühzeitig durch die Geschäftsführung beteiligt.

Ein Meldeformular steht auf der Homepage der/des Berliner Landesbeauftragten für den Datenschutz und die Informationsfreiheit zur Verfügung:

https://www.datenschutz-berlin.de/wirtschaft-und-verwaltung/meldung-einer-datenpanne/

4.5 Dokumentation im JC

Alle Verletzungen des Schutzes personenbezogener Daten **sind zwingend zu dokumentieren,** um die gesetzliche Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO einzuhalten. Dazu ist der Fall durch die/den Mitarbeiter*in in Datenschutzangelegenheiten bzw. den gesondert zu bestimmenden Mitarbeiter*innen des Teams 647 in unterstützender fachlicher Vertretung in die Datenbank für Datenschutzfälle einzutragen:

Dokumentation

Die Datenbank gewährleitstet dabei die direkte Anbindung an die verantwortliche Geschäftsführung und stellt darüber hinaus sicher, dass die gesetzlichen Fristen hinreichend beachtet werden. Die Zugriffe auf die Datenbank sind auf die Geschäftsführung, die die/den Mitarbeiter*in in Datenschutzangelegenheiten und die gesondert zu bestimmenden Mitarbeiter*innen des Teams 647 in unterstützender fachlicher Vertretung, deren Team- und zuständige Bereichsleitung, die/den bDSB und temporär zur technischen Wartung auf maximal zwei IT-Speziallisten beschränkt.

Die Arbeitshilfe zur Bedienung der Datenbank befindet sich unter dem nachfolgenden Link und liegt dieser GA zusätzlich als Anlage E bei.

Nach Rücklauf der Bearbeitung durch die zuständige Teamleitung per E-Mail an das Postfach

Jobcenter-Berlin-Neukoelln.Datenschutzmeldung@jobcenter-ge.de

und der abschließenden Beurteilung und Meldung an die zuständigen Stellen (z.B. Stabsstelle Datenschutz bzw. BMAS und BfDI) erfolgt die abschließende Dokumentation in der genannten Tabelle durch die/den Mitarbeiter*in in Datenschutzangelegenheiten bzw. den gesondert zu bestimmenden Mitarbeiter*innen des Teams 647 in unterstützender fachlicher Vertretung. Zur fachlichen Unterstützung kann die/der bDSB hinzugezogen werden.

In der (Dokumentations-) Ablage

\\Dst.baintern.de\dfs\922\Ablagen\D92202-GL-FK\17_Datenschutzmeldung\Dokumentation der einzelnen Meldungen

ist zusätzlich unter dem Datum der Kenntniserlangung ein Ordner anzulegen, in dem die Mitteilung (z.B. schriftliche Anzeige oder E-Mail des SC, eines Kunden, Mitarbeiter*in oder Dritten) der Verletzung des Schutzes personenbezogener Daten der bzw. die Meldebögen, die Meldungen (E-Mail) an die Stabsstelle Datenschutz bzw. die Aufsichtsbehörden, etwaige Antworten und sonstiger Schriftwechsel zu speichern sind. Hierzu gehört ggf. auch eine Kopie über die schriftliche Information nach Art. 34 DSGVO an die/den Betroffene/n bzgl. der Datenschutzverletzung.

Die Zugriffe auf diese Ablage sind auf die Geschäftsführung, die/den Mitarbeiter*in in Datenschutzangelegenheiten und den gesondert zu bestimmenden Mitarbeiter*innen des Teams 647 in unterstützender fachlicher Vertretung, deren Team- und zuständige Bereichsleitung, die/den bDSB und deren/dessen Vertretung beschränkt.

Die Speicherung der Vorgänge in der Ablage und der Datenbank ist zulässig, soweit und solange die Daten zur Nachweisführung im Rahmen der Rechenschaftspflicht der Verantwortlichen im Einzelfall erforderlich sind. Die Erforderlichkeit liegt innerhalb eines laufenden Leistungsbezuges dauerhaft vor. Wird der Leistungsbezug beendet, erfolgt eine Überprüfung der Erforderlichkeit erstmals 12 Monate nach Beendigung des Leistungsbezuges.

Sofern die Erforderlichkeit zur Speicherung entfällt, sind die Daten zu löschen.

Sowohl die Datenbank als auch die Datenablage sind in das Verzeichnis von Verarbeitungstätigkeiten (VVT) aufzunehmen.

Soweit die Meldung an die jeweils zuständigen Stellen (Stabsstelle Datenschutz oder BfDI und BMAS) durch die/den Mitarbeiter*in in Datenschutzangelegenheiten bzw. die/den gesondert zu bestimmenden Mitarbeiter*innen des Teams 647 in unterstützender fachlicher Vertretung erfolgt ist, wird die jeweils zuständige Team- und Bereichsleitung, welche den Sachverhalt ermittelt und den Meldebogen an das Funktionspostfach übermittelt hat, über den Abschluss des Verfahrens informiert und zur Löschung des bis dahin gespeicherten Meldebogens aufgefordert.

Die jeweilige Teamleitung zeigt die Löschung des Meldebogens über das folgende Postfach verschlüsselt an:

Jobcenter-Berlin-Neukoelln.Datenschutzmeldung@jobcenter-ge.de.

5. Datenschutz und IT-Sicherheit

Die Einhaltung des Datenschutzes sowie der IT-Sicherheit ist durch alle Mitarbeiter*innen zu gewährleisten.

Löschung der Meldung bei der zuständigen Teamleitung

Der Zugriff auf die Datenbank, die Dokumentationsablage und das E-Mail-Postfach Jobcenter-Berlin-Neukoelln.Datenschutzmeldung@jobcenter-ge.de ist auf die Geschäftsführung, die/den Mitarbeiter*in in Datenschutzangelegenheiten und die gesondert zu bestimmenden Mitarbeiter*innen des Teams 647 in unterstützender fachlicher Vertretung, deren Team- und zuständige Bereichsleitung, die/den bDSB und deren/dessen Vertretung beschränkt.

Bezüglich der Datenbank wird bei Bedarf, temporär zur technischen Wartung, ein weiterer temporärer Zugriff von maximal zwei IT-Speziallisten eingerichtet und nach Abschluss der Arbeiten entsprechend wieder entfernt.

Die Zugriffsberechtigungen auf die Dokumentation der Datenschutzverletzungen (Ablage, das E-Mail-Postfach und die Datenbank) sind restriktiv und nur nach Abstimmung mit dem bDSB zu vergeben.

6. Schulung

Die/Der Mitarbeiter*in in Datenschutzangelegenheiten und die gesondert zu bestimmenden Mitarbeiter*innen des Teams 647 in unterstützender fachlicher Vertretung, die für diese Aufgabenwahrnehmung durch die Geschäftsführung bestimmt bzw. beauftragt wurden und alle Bereichsleitungen erhalten durch die/den bDSB eine entsprechende fachliche Einarbeitung. Zusätzlich erfolgt eine enge fachliche Begleitung bei der Aufgabenwahrnehmung in den ersten drei Monaten nach Gültigkeit dieser GA durch die/den bDSB.

7. Schlussbestimmungen /Inkrafttreten

Diese Weisung tritt mit Unterzeichnung und Veröffentlichung in Kraft.

Berlin, den 05.10.2021

gez.
Dr. Brendel
Geschäftsführer

Anlage A - Kurzpapier Nr.18 der Datenschutzkonferenz (DSK)

Anlage B - Meldebogen intern (wird in dieser Form sowohl für die interne Erfassung, als auch für die Datenschutz-Meldung an die Stabsstelle Datenschutz in der Zentrale der BA verwendet)

Anlage C - Erläuterung aus der Zentrale zum (internen) Meldebogen der BA

Anlage D - Meldebogen BMAS und BfDI

Anlage E - Arbeitshilfe Datenbank-Datenschutzfälle

Ablage F - Ablaufschema zur Meldung von Datenschutzfällen