Bundesamt
für Soziale Sicherung

Bundesamt für Soziale Sicherung, Friedrich-Ebert-Allee 38, 53113 Bonn

An alle
bundesunmittelbaren
Sozialversicherungsträger

sowie deren Datenschutzbeauftragte

- nur per E-Mail -

HAUSANSCHRIFT
Friedrich-Ebert-Allee 38
53113 Bonn

TEL +49 228 619 1944

referat117@bas.bund.de
www.bundesamtsozialesicherung.de

BEARBEITER(IN) FRAU SCHIPPEL

21. April 2020

AZ 117 – 8240 – 2075/2017
(bei Antwort bitte angeben)

nachrichtlich:
Bundesministerium für Arbeit und Soziales – BMAS, Referat IVa1

Bundesministerium für Gesundheit – BMG, Referat 211

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit - BfDI, Referat 13

Ministerien und Senatsverwaltungen für Gesundheit und Soziales der Länder

Datenschutz im Aufsichtsbereich – hier: Meldung einer Datenschutzverletzung nach § 83a SGB X i. V. m. Artikel 33 DSGVO

Rundschreiben, Meldevordruck und Bearbeitungshinweise

Sehr geehrte Damen und Herren,

mit Anwendung der DSGVO haben wir bereits mehrere Rundschreiben zur Meldung von Datenschutzverletzungen veröffentlicht, zuletzt mit Schreiben vom 22. Mai und 8. Juni 2018. Die in der Aufsichtspraxis laufend neu gewonnenen Erkenntnisse geben uns Anlass, den Meldevordruck anzupassen sowie weitere Bearbeitungshinweise zu erstellen. Beides übersenden wir in der aktuellsten Version.

Insbesondere haben wir Unsicherheiten bei der Risikoanalyse festgestellt. Wir weisen in diesem Zusammenhang darauf hin, dass die in unserem Rundschreiben vom 8. Juni 2018 erläuterte dreistufige Risikoklassifizierung erhalten bleibt:

Risikoklasse	Meldepflicht und Benachrichtigungspflicht
geringes Risiko	Keine Meldepflicht gegenüber dem Bundesamt für Soziale Sicherung (BAS) gemäß § 83a SGB X, aber Dokumentationspflicht gemäß Artikel 33 Absatz 5 DSGVO für die Verantwortlichen.
Risiko	Meldepflicht gegenüber dem BAS gemäß § 83a SGB X, aber keine Mitteilungspflicht gegenüber den Betroffenen gemäß Artikel 34 DSGVO.
hohes Risiko	Meldepflicht gegenüber dem BAS gemäß § 83a SGB X und Mitteilungspflicht gegenüber den Betroffenen gemäß Artikel 34 DSGVO.

Um bei der unbedingt von den Verantwortlichen vorzunehmenden Risikoabwägung eine Hilfestellung zu geben, haben wir den Mustervordruck um Bewertungsstufen ergänzt:

Risikoanalyse

Wie wird das voraussichtliche Risiko für die betroffenen Personen beurteilt?

a) Schwere des Schadens für die betroffenen Personen ☐ 1 ☐ 2 ☐ 3

b) Wahrscheinlichkeit des Eintritts des Schadens ☐ 1 ☐ 2 ☐ 3

Aus den Bewertungen a) und b) ergibt sich nach dem Vorsichtsprinzip folgende Einschätzung:

☐ 1 - geringes Risiko — Keine Meldepflicht, aber Dokumentationspflicht

☐ 2 - Risiko — Meldepflicht, aber keine Mitteilungspflicht gegenüber Betroffenen

☐ 3 - hohes Risiko — Meldepflicht und Mitteilungspflicht gegenüber Betroffenen

Erfolgte die Meldung innerhalb von 72 Stunden?

☐ Ja

☐Nein

Weitere Erläuterungen:

Weitere Erläuterungen hier eintragen, falls „Nein“ ausgewählt wurde

Wir empfehlen bei der Risikoanalyse nach dem Vorsichtsprinzip vorzugehen. Sobald aufgrund der Analyse die Schwere des Schadens oder die Eintrittswahrscheinlichkeit in einer der beiden Kategorien 2 (Risiko) oder 3 (hohes Risiko) eingeordnet wird, ist die Meldepflicht

gegenüber dem BAS gegeben. Wird Beides (Schadensschwere und Eintrittswahrscheinlichkeit) in die Kategorie 3 (hohes Risiko) eingeordnet, tritt zudem die Mitteilungspflicht gegenüber den Betroffenen hinzu.

Ergänzend verweisen wir auch auf das Papier der Datenschutzkonferenz (DSK) Kurzpapier - Nr. 18 (Risiko für die Rechte und Freiheiten natürlicher Personen, Stand: 26.04.2018; https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf). Hier wird insbesondere auf die auf Seite 5 dargestellte Risikomatrix sowie den darauffolgenden Absatz hingewiesen. Damit wird klar, dass es Fälle geben kann, die nicht meldepflichtig sind, aber auch Fälle, die trotz geringer Eintrittswahrscheinlichkeit, aber einer schwerwiegenden Schadensmöglichkeit - oder auch umgekehrt - in die Kategorie „hohes Risiko“ fallen.

Auf die Notwendigkeit, anlässlich der Datenschutzverletzung eine Risikoanalyse durch die verantwortliche Stelle vorzunehmen, möchten wir nochmals hinweisen, da dieses Verfahren Hinweise für die eigene kontinuierliche Überprüfung der eigenen Schutzmaßnahmen geben kann. Die Berücksichtigung der Erkenntnisse aus der Analyse der Datenschutzverletzungen kann z. B. in einen kontinuierlichen Verbesserungsprozess (sog. Plan-Do-Check-Act-Zyklus) einfließen.

Denn bei der Datenverarbeitung müssen nach den Vorgaben der DSGVO die technischen und organisatorischen Schutzmaßnahmen angemessen und geeignet sein, die Risiken für die Rechte und Freiheiten der von der Verarbeitung betroffenen Personen soweit einzudämmen, dass ein dem Risiko angemessenes Schutzniveau gewährleistet sowie das entstehende Risiko gemindert wird.

Wir empfehlen für die Meldung von Datenschutzverletzungen weiterhin die Verwendung eines strukturierten Meldevordrucks, weil dadurch eine aufwendige Nachverfolgung für beide Seiten vermieden werden kann. Wie bekannt, finden Sie das Rundschreiben, den Meldevordruck und die weiteren Bearbeitungshinweise zum Download auf unserer Internetseite unter: https://www.bundesamtsozialesicherung.de/de/themen/alle-sozialversicherungszweige-informationstechnik-und-datenschutz/ueberblick/

Überdies bitten wir Sie, die für die Meldung von Datenschutzverletzungen eingerichteten E-Mail-Funktionspostfächer zu nutzen:
Datenschutzverletzung(at)bas.bund.de
Datenschutzverletzung(at)bas.de-mail.de

Informationen zur verschlüsselten Kommunikation mit dem Bundesamt für Soziale Sicherung finden Sie auf unserer Internetseite unter:
https://www.bundesamtsozialesicherung.de/de/bundesamt-fuer-soziale-sicherung/kontakt/e-mail-verschluesselung/
https://www.bundesamtsozialesicherung.de/de/bundesamt-fuer-soziale-sicherung/kontakt/de-mail/

Selbstverständlich können Sie uns Ihre Meldungen auch weiterhin postalisch übersenden. Von einer Übersendung per Fax bitten wir aus datenschutzrechtlicher Sicht abzusehen.

Bei Rückfragen sowie Anregungen stehen wir Ihnen auf gewohntem Wege zur Verfügung.

Mit freundlichen Grüßen
Im Auftrag
gez. (Schlotter)

Anlagen
- Meldevordruck (Version_2.0)
- Bearbeitungshinweise (Version_2.0)