Bearbeitungshinweise zum Meldevordruck Datenschutzverletzung Version_2.0
(§ 83a SGB X i. V. m. Artikel 33 DSGVO)

Was ist eine Datenschutzverletzung?

Eine Datenschutzverletzung ist ein Ereignis, das den Schutz bzw. die Sicherheit der personenbezogenen Daten betrifft. Auch die unrechtmäßige Verarbeitung oder eine Verarbeitung nicht entsprechend der DSGVO-Grundsätze (Artikel 4 Nr. 12 und Artikel 5 DSGVO) stellt eine Verletzung dar. Dabei ist unerheblich, ob das Ereignis versehentlich, geplant oder ohne Erlaubnis erfolgt. Außer der Verletzung können weitere Risiken bzw. Folgeschäden entstehen.

- Die **Datenverfügbarkeit** wird z. B. verletzt, wenn die zu verarbeitenden Daten verloren gehen, vernichtet werden oder nicht verlässlich abgerufen werden können. Die Datenverfügbarkeit kann z. B. durch Überlastung der Technik, Schadstoffsoftware, Sabotage, Hacking beeinflusst werden.

- Die **Datenintegrität** wird z. B. verletzt, wenn die zu verarbeitenden Daten nicht mehr unversehrt, vollständig, richtig und aktuell sind. Veränderungsmöglichkeiten müssen ausgeschlossen werden oder feststellbar bzw. dokumentiert sein, damit Veränderungen beachtet oder korrigiert werden können. Die Datenintegrität kann z. B. durch eine Überlastung der Systeme oder auch durch fehlerhafte Speicherrechte beeinflusst werden.

- Die **Datenvertraulichkeit** wird z. B. verletzt, wenn unbefugte Personen die Daten zur Kenntnis nehmen oder nutzen können, Daten unrechtmäßig verknüpft oder verkettet werden. Unbefugte Personen können neben Dritten auch Mitarbeitende der verantwortlichen Stelle sein, wenn diese den Zugriff auf die Daten nicht benötigen.

Welche Folgen bzw. welchen Schaden kann eine Datenschutzverletzung haben?

Eine Datenschutzverletzung kann u. a.

- das Grundrecht auf Datenschutz verletzen,
- zu einem materiellen, immateriellen oder physischen Schaden oder
- auch zu Folgeschäden für die betroffene(n) Person(en) führen,

wenn nicht rechtzeitig und angemessen vom Verantwortlichen reagiert wird.

Zu den sich aus der Verletzung ergebenden möglichen Schäden gehört z. B.: der Verlust der Kontrolle über die Daten, die Verarbeitung wider Treu und Glauben, die Verwendung nach der Löschfrist, die Verarbeitung falscher Daten, die fehlende Wiederherstellbarkeit oder Korrektur der Daten, der Identitätsdiebstahl oder -betrug, die Ruf- und Imageschädigung, die missbräuchliche Nutzung der eGK, Geheimnisoffenbarung, Folgeschaden (wirtschaftliche oder gesellschaftliche Nachteile), der Verlust des Arbeitsplatzes, Nachteile beim Abschluss privater Versicherungen oder auch die Nichterfüllung der Betroffenenrechte bzw. fehlende Unterstützung. Die vorgenannte Aufzählung erhebt keinen Anspruch auf Vollständigkeit.

Wie ist die Risikolage zu beurteilen?

Maßgebend für die Beurteilung der Verletzung ist die sog. Risikoanalyse. Nach dem risikobasierten Ansatz wird

- die Schwere des Schadens für die betroffene(n) Person(en) und
- die Wahrscheinlichkeit des Eintritts des Schadens beurteilt.

Je größer beides anzusehen ist, desto höher ist die Risikostufe einzuschätzen. Dabei können ähnliche Ereignisse kontextbezogen zu unterschiedlichen Beurteilungen führen.

Welche Risikoklassen, Dokumentations-, Melde- und Informationspflichten gibt es?

Die Risikoklassifizierung haben wir in unserem Rundschreiben vom 8. Juni 2018 erläutert und wird hier nur kurz dargestellt:

„geringes Risiko“	keine Meldepflicht gegenüber dem BAS, aber Dokumentationspflicht des Verantwortlichen (Artikel 33 Absatz 5 DSGVO)
„Risiko“	Meldepflicht gegenüber dem BAS, aber keine Informationspflicht gegenüber betroffenen Personen (Artikel 33 Absatz 1 und Artikel 34 DSGVO)
„hohes Risiko“	Kombination aus Melde- und Informationspflicht (Artikel 33 Absatz 1 und Artikel 34 DSGVO)

Eine vollständig risikolose Datenverarbeitung gibt es nicht. Daher ist die erste Risikoklasse als „geringes Risiko“ bezeichnet. Die aufgrund der Risikoanalyse ermittelte Risikoklasse entscheidet somit über die Dokumentations-, Melde- und Informationspflichten.

Wie kann die Risikoanalyse angegeben werden?

Für die Abgabe der Risikoanalyse haben wir den Meldevordruck um eine Visualisierung unter Verwendung der Risikoklassen ergänzt, welche die allgemeine Regel widerspiegelt (Erwägungsgrund 75, 76 und 94 Satz 2):

Risiko = Schadensschwere * Eintrittswahrscheinlichkeit

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 daher 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 Personen hinzu.

Wann ist eine Datenschutzverletzung zu melden?

Artikel 33 DSGVO stellt darauf ab, dass Datenschutzverletzungen zu melden sind, *„es sei denn, dass die Verletzung des Schutzes der personenbezogenen Daten voraussichtlich **nicht** zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt“*.

Gibt es eine Meldefrist?

Liegt eine Datenschutzschutzverletzung vor und ist nach der Risikoanalyse eine Meldung abzugeben, so hat diese unverzüglich, mindestens innerhalb von 72 Stunden nach Bekanntwerden zu erfolgen (Artikel 33 Absatz 1 und 4 DSGVO). Je höher die Risikostufe ist, umso wichtiger ist es, schnell und angemessen zu reagieren und entsprechende Maßnah-

men zu ergreifen. Wird die Frist **nicht** eingehalten, **müssen** die Gründe bei der Meldung angegeben werden (vgl. Artikel 33 Absatz 1 DSGVO).

Wer ist Verantwortlicher für die Datenverarbeitung?
Verantwortlicher ist nach der DSGVO „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.“ (Artikel 4 Nr. 7 DSGVO). Bundesunmittelbare Sozialversicherungsträger sind unabhängig von ihrer Organisation verantwortlich, denn sie verarbeiten und entscheiden über Sozialdaten im Rahmen ihrer Aufgaben.

Was ist die Aufgabe des Verantwortlichen?
Eine Aufgabe des Verantwortlichen ist es, die Risiken und Schutzbedarfe der Datenverarbeitung zu identifizieren, zu analysieren und einzustufen und Maßnahmen zu deren Eindämmen zu treffen.

Was sind „geeignete technische und organisatorische Maßnahmen“?
Grundsätzlich gilt, je höher das Risiko desto höher ist der Schutzbedarf für die Datenverarbeitungsprozesse und desto höhere Ansprüche sind an die geeigneten technischen und organisatorischen Maßnahmen zu stellen. Dabei sind die Maßnahmen so auszuwählen, dass sie die nach der DSGVO geltenden Grundsätze für die Datenverarbeitung erfüllen (Artikel 5 DSGVO). Hinsichtlich der Einhaltung dieser Grundsätze sind Verantwortliche rechenschaftspflichtig (Artikel 5 Absatz 2 DSGVO).

Die nach diesen Grundsätzen initialisierten Maßnahmen erfordern eine ständige Kontrolle und Verbesserung (sog. Plan-Do-Check-Act-Zyklus). Die Verbesserung der Maßnahmen verändert nicht den Schutzbedarf, aber die Eintrittswahrscheinlichkeit und damit insgesamt den Risikowert.

Ein verbindlicher Prozess zur Feststellung, Meldung, Behebung und Abmilderung von Datenschutzverletzungen, ein Rechte-/Rollenkonzept, Vertretungsregelungen oder auch die Sensibilisierung und Schulung der Beschäftigten stellen beispielsweise sog. Maßnahmen dar.