Vorbemerkung

Mit dem Geltungsbeginn der DS-GVO und des BDSG neu ergeben sich im Falle einer Datenschutzverletzung Informationspflichten gegenüber den Aufsichtsbehörden und den Betroffenen aus Art. 33 und 34 DS-GVO.

Dabei ist im Einzelnen Folgendes zu beachten:

- Kommt es beim DRK Kreisverband Odenwaldkreis e. V. zu einer Datenschutzverletzung hinsichtlich Personenbezogener Daten, bzw. wird eine bekannt, ist diese sowohl dem unmittelbar Dienstvorgesetzten, als auch dem Datenschutzbeauftragten (DSB) zu melden.
- Dies kann formlos geschehen.
- Der DSB bearbeite den Vorfall und unternimmt die weiteren Schritte in Absprache mit den Verantwortlichen (GL).

Definition von Datenschutzverletzung

Art. 4 Nr. 12 DS-GVO definiert den Begriff *„Verletzung des Schutzes personenbezogener Daten*" als eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder 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. Eine Verletzung der Sicherheit liegt demnach vor, wenn in Bezug auf personenbezogene Daten

- Vernichtung,
- Verlust,
- Veränderung eintreten oder
- eine unbefugte Offenlegung oder
- ein unbefugter Zugang erfolgt.

Darüber hinaus tritt eine Verletzung der Sicherheit bereits ein, wenn ein unbefugter Zugang zu personenbezogenen Daten, z.B. durch den Verlust eines Datenträgers, möglich erscheint. Es ist nicht erforderlich, dass eine unbefugte Kenntnisnahme tatsächlich erfolgt ist. Für eine Verletzung des Schutzes personenbezogener Daten ist ein Verschulden im Sinne von Vorsatz oder Fahrlässigkeit nicht erforderlich. Die Definition umfasst ausdrücklich sowohl unbeabsichtigtes, als auch gezieltes Handeln.

Meldepflicht gegenüber den **Aufsichtsbehörden** (Art. 33 DS-GVO)

Die Meldung von Verletzungen des Schutzes personenbezogener Daten gegenüber der zuständigen Aufsichtsbehörde richtet sich nach Art. 33 DS-GVO.

1. Meldepflichtige Ereignisse

Gemäß Art. 33 Abs. 1 Satz 1 DS-GVO ist der Verantwortliche verpflichtet,

- eine Verletzung des Schutzes personenbezogener Daten der zuständigen Aufsichtsbehörde zu melden,
- es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen.
    - dieses zu beurteilen liegt im Verantwortungsbereich des Verantwortlichen und des DSB

Der Verantwortliche hat diesbezüglich eine Prognoseentscheidung über die möglichen Auswirkungen der festgestellten Schutzverletzung vorzunehmen.

Das Risiko für die Rechte und Freiheiten natürlicher Personen ist unter Berücksichtigung der Eintrittswahrscheinlichkeit und der möglichen Schadensschwere zu ermitteln.

Es ist von einem hohen Risiko jedenfalls dann auszugehen, wenn

- besondere Kategorien von Daten nach Art. 9 oder Art. 10 DS-GVO (Gesundheitsdaten),
- personenbezogene Daten, die einem Berufsgeheimnis unterliegen oder
- personenbezogene Daten zu Bank- oder Kreditkartenkonten

unrechtmäßig übermittelt wurden oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind und aus diesem Grund schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der betroffenen Personen drohen.7

Anhaltspunkte, worin im Einzelnen das Risiko für die Rechte und Freiheiten natürlicher Personen bestehen kann, sind:

- der Verlust der Kontrolle über die personenbezogenen Daten,
- eine Einschränkung von Rechten,
- Diskriminierung,
- Identitätsdiebstahl oder -betrug,
- finanzielle Verluste,
- die unbefugte Aufhebung einer Pseudonymisierung,
- eine Rufschädigung,
- den Verlust der Vertraulichkeit von Daten, die dem Berufsgeheimnis unterliegenden, oder
- andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die

2.Zuständige Aufsichtsbehörde

Die Meldung muss gegenüber der zuständigen Aufsichtsbehörde erfolgen. Die Bestimmung der Zuständigkeit richtet sich nach Art. 55 und 56 DS-GVO.

Die Zuständigkeit ergibt sich grundsätzlich aus dem Ort der Datenverarbeitung.

Im „Normalfall" ist für den DRK Kreisverband Odenwaldkreis e.V. die zuständige Aufsichtsbehörde der Hessische Beauftragte für Datenschutz und Informationsfreiheit (https://www.datenschutz.hessen.de)

3.Meldefrist

Gemäß Art. 33 Abs. 1 Satz 1 DS-GVO ist der Verantwortliche verpflichtet, der zuständigen Aufsichtsbehörde die Verletzung unverzüglich und spätestens binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, zu melden. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, ist ihr eine Begründung für die Verzögerung beizufügen (Art. 33 Abs. 1 Satz 2 DS-GVO).

Für den Fristbeginn reicht demnach der bloße Verdacht einer Verletzung nicht aus. Eine Meldepflicht besteht aber auch nicht erst dann, wenn die Verletzung durch den Verantwortlichen positiv festgestellt wurde.

Es ist davon auszugehen, dass die Meldefrist zu laufen beginnt, wenn aufgrund tatsächlicher Anhaltspunkte eine hohe Wahrscheinlichkeit für eine Verletzung besteht.

Nach Fristbeginn muss die Meldung an die Aufsichtsbehörde unverzüglich erfolgen. Inhalt und Form der Meldung

4.Der Mindestinhalt

Der Mindestinhalt der Meldung an die Aufsichtsbehörde ergibt sich aus Art. 33 Abs. 3 DS-GVO:

- Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten (Art. 33 Abs. 3a DS-GVO),
- soweit möglich, Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Datenkategorien und der ungefähren Zahl der betroffenen Datensätze (Art. 33 Abs. 3a DS-GVO),
- den Namen und die Kontaktdaten des Datenschutzbeauftragten (Art. 33 Abs. 3b DS-GVO),
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten (Art. 33 Abs. 3c DS-GVO),
- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Datenschutzverletzung und gegebenen- falls zur Abmilderung ihrer möglichen nachteiligen Auswirkungen (Art. 33 Abs. 3d DS-GVO).

Die Informationen sollen der Aufsichtsbehörde eine Prüfung ermöglichen, ob die getroffenen Maßnahmen ausreichen, damit die Behörde im Bedarfsfall selbst geeignete Maßnahmen anordnen kann.

Auch wenn eine gesetzliche Pflicht hierzu nicht besteht, sollte bei der Meldung einer Datenschutzverletzung gegenüber der Aufsichtsbehörde der Datenschutzbeauftragte immer eingebunden werden.

Für die Meldung an die Aufsichtsbehörde ist das Meldeformular des Hessischen Beauftragten für Datenschutz und Informationsfreiheit (https://www.datenschutz.hessen.de) zu verwenden:

- https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2022-11/hbdi_formular_art33.docx

5. Dokumentationspflichten

Gemäß Art. 33 Abs. 5 DS-GVO dokumentiert der Verantwortliche Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, die Auswirkungen der Verletzung und die ergriffenen Abhilfemaßnahmen.

Diese Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Vorgaben von Art. 33 DS- GVO ermöglichen.

6. Unterstützungspflicht des Auftragsverarbeiters

Art. 33 Abs. 2 DS-GVO sieht eine originäre Pflicht des Auftragsverarbeiters vor, den Verantwortlichen unverzüglich zu informieren, wenn ihm eine Datenschutzverletzung bekannt wird. Eine zusätzliche Meldepflicht gegenüber der Aufsichtsbehörde hat der Auftragsverarbeiter jedoch nicht.

Der Auftragsverarbeiter muss dem Verantwortlichen jede Datenschutzverletzung melden.

Für den Auftragsverarbeiter beginnt die Informationspflicht ebenfalls mit dem Vorliegen tatsächlicher Anhaltspunkte, die mit hoher Wahrscheinlichkeit auf eine Datenschutzverletzung schließen lassen.

7. Sanktionen

Bei einem Verstoß gegen die Meldepflicht gegenüber der Aufsichtsbehörde können gemäß Art. 83 Abs. 4a DS-GVO Geldbußen von bis zu 10.000.000 Euro oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden, je nachdem, welcher der Beträge höher ist. Die Geldbußen können zusätzlich zu oder anstelle der in Art. 58 Abs. 2 DS-GVO normierten umfangreichen Abhilfebefugnisse der Aufsichtsbehörden verhängt werden (Art. 58 Abs. 2i DS-GVO).

Meldepflicht gegenüber der betroffenen Person (Art. 34 DS-GVO)

Der Verantwortliche ist gemäß Art. 34 DS-GVO verpflichtet, bei Datenschutzverletzungen unter bestimmten Voraussetzungen auch die betroffene Person zu benachrichtigen.

1. Benachrichtigungspflichtiges Ereignisse

Gemäß Art. 34 Abs. 1 DS-GVO benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung, wenn die Verletzung des Schutzes personenbezogener Daten **voraussichtlich ein hohes Risiko** für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat.

2. Meldefrist

Gemäß Art. 34 Abs. 1 DS-GVO sind die betroffenen Personen „unverzüglich" zu informieren. Bei dem Begriff der „Unverzüglichkeit" sind jedoch andere Maßstäbe als bei der Meldung gegenüber der Aufsichtsbehörde anzulegen. Die Benachrichtigung der betroffenen Person soll stets so rasch wie nach allgemeinem Ermessen möglich, in enger Absprache mit der Aufsichtsbehörde und nach Maßgabe der von dieser oder von anderen zuständigen Behörden, wie beispielsweise Strafverfolgungsbehörden, erteilten Weisungen erfolgen. Eine längere Benachrichtigungsfrist kann gerechtfertigt sein, wenn es darum geht, geeignete Maßnahmen gegen fortlaufende oder vergleichbare Verletzungen des Schutzes personenbezogener Daten zu treffen.
Eine Frist von 72 Std. Frist sollte nach Möglichkeit eingehalten werden

3. Inhalt und Form der Meldung

Gemäß Art. 34 Abs. 2 DS-GVO hat der Verantwortliche die Art der Datenschutzverletzung in klarer und einfacher Sprache zu beschreiben. Darüber hinaus müssen zumindest die in Art. 33 Abs. 3b, c und d DS-GVO genannten Informationen und Maßnahmen enthalten sein:

- Name und Kontaktdaten des Datenschutzbeauftragten,
- Beschreibung der wahrscheinlichen Verletzungsfolgen sowie
- Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Datenschutzverletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

4. Ausnahmen von der Benachrichtigungspflicht

Art. 34 Abs. 3 DS-GVO und § 29 Abs. 1 Satz 3 und 4 BDSG neue Fassung enthalten Ausnahmefälle, in denen eine Benachrichtigung der betroffenen Person entfallen kann:

a) Geeignete technisch-organisatorische Sicherheitsvorkehrungen

Der Verantwortliche hat geeignete technisch-organisatorische Sicherheitsvorkehrungen getroffen, die auf die Datenschutzverletzung angewandt wurden, insbesondere solche, durch welche die personenbezogenen Daten für Unbefugte unverständlich gemacht wurden, etwa durch Verschlüsselung (Art. 34 Abs. 3a DS-GVO).

b) Nachträgliche Maßnahmen des Verantwortlichen zur Risikominimierung

Der Verantwortliche hat nach der Datenschutzverletzung, aber vor einer etwaigen Benachrichtigung bereits durch entsprechende Maßnahmen sichergestellt, dass ein hohes Risiko für die Rechte und Freiheiten der jeweils betroffenen Personen aller Wahrscheinlichkeit nach nicht mehr besteht (Art. 34 Abs. 3b DS-GVO).

c) Öffentliche Bekanntmachung anstelle der Benachrichtigung

Wenn eine Benachrichtigung mit einem unverhältnismäßigen Aufwand verbunden wäre, hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden (Art. 34 Abs. 3c DS-GVO).

d) Ausnahme gemäß § 29 Abs. 1 Satz 3 und 4 BDSG neue Fassung

Die Pflicht zur Benachrichtigung gemäß Art. 34 DS-GVO besteht gemäß § 29 Abs. 1 Satz 3 BDSG neue Fassung nicht, soweit durch die Benachrichtigung Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. Abweichend davon ist die betroffene Person jedoch gemäß § 29 Abs. 1 Satz 4 BDSG neue Fassung zu benachrichtigen, wenn die Interessen der betroffenen Person, insbesondere unter Berücksichtigung drohender Schäden, gegenüber dem Geheimhaltungsinteresse überwiegen.

5. Sanktionen

Bei einem Verstoß gegen die Meldepflicht gegenüber der betroffenen Person können gemäß Art. 83 Abs. 4a DS-GVO Geldbußen von bis zu 10.000.000 Euro oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden, je nachdem, welcher der Beträge höher ist. Die Geldbußen können zusätzlich zu oder anstelle der in Art. 58 Abs. 2 DS-GVO normierten umfangreichen Abhilfebefugnisse der Aufsichtsbehörden verhängt werden (Art. 58 Abs. 2i DS-GVO).