Vorgehen bei Datenschutzverletzungen

Deutsches Rotes Kreuz
Kreisverband Odenwaldkreis e.V.

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

Mitgeltendes Dokument: „VA Vorgehen bei DS Verletzungen“

1. Checkliste

Aus den vorstehenden Ausführungen ergibt sich für den DRK KV folgende empfohlene Vorgehensweise in Form einer Checkliste:

a. Liegen Anhaltspunkte für eine Verletzung des Schutzes personenbezogener Daten vor?

☐ Angriff auf das Computersystem von außen, z. B. durch Viren oder Trojaner

☐ Verlust von Laptops, Smartphones, USB-Sticks, externen Festplatten oder Sicherungsbändern

☐ Diebstahl eines Smartphones oder eines IT Systems (PC, Notebook, Laptop, Tablet)

☐ unbefugtes Weitergeben von Daten durch Mitarbeiter

☐ unzulässige Nutzung personenbezogener Daten

☐ Einbruch in bzw. unbefugter Zutritt in Räumlichkeiten, in denen personenbezogene Daten aufbewahrt werden

☐ Sonstiges: _____

Ist das Ereignis:

☐ „Bekanntgeworden“ (tatsächliche Anhaltspunkte, hohe Wahrscheinlichkeit)

b. Besteht dadurch ein Risiko für die Rechte und Freiheiten natürlicher Personen?

- Erfordert Risikoabwägung (Prognose über mögliche Auswirkungen unter Berücksichtigung von Eintrittswahrscheinlichkeit und möglicher Schadensschwere)

  Im Sozial und Gesundheitsbereich ist grundsätzlich davon auszugehen, dass ein meldepflichtiges Ereignis vorliegt, wenn personenbezogene Patientendaten unrechtmäßig an Dritte übermittelt wurden oder Dritte diese auf sonstige Weise unrechtmäßig zur Kenntnis nehmen konnten

- **Falls nein: Keine Informationspflicht gegenüber der Aufsichtsbehörde, aber Dokumentationspflicht gemäß Art. 33 Abs. 5 DS-GVO!**

c. Inhalt der Meldung: siehe Art. 33 Abs. 4 DS-GVO

- ☐ Art der Verletzung
- ☐ Kategorien und ungefähre Anzahl betroffener Personen
- ☐ Name und Kontaktdaten des betrieblichen Datenschutzbeauftragten
- ☐ wahrscheinliche Verletzungsfolgen
- ☐ ergriffene oder vorgeschlagene Maßnahmen

☐ Zeitpunkt der Meldung: unverzüglich (ohne schuldhaftes Zögern) spätestens aber innerhalb von 72 Stunden (beachte: Meldung innerhalb von 72 Stunden dennoch verspätet, wenn sie nicht „unverzüglich“ abgegeben wurde!)

- falls Zeitspanne von 72 Stunden nicht eingehalten wird, Begründung für Verzögerung notwendig (Art. 33 As. 1 Satz 2 DS-GVO)

☐ falls noch nicht alle Informationen vorliegen, schrittweise Information erforderlich (Art. 33 Abs. 4 DS-GVO)

☐ Form: möglichst in Textform und möglichst über bereitgestelltes Formular des hessischen Beauftragten für Datenschutz und Informationsfreiheit:

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

☐ in dringenden Fällen auch telefonisch möglich (dann Telefonat dokumentieren und Meldung in Textform so schnell wie möglich nachholen)

☐ Zuständige Aufsichtsbehörde:

- Hessischer Beauftragter für Datenschutz und Informationsfreiheit (Aufsichtsbehörde (Landesdatenschutzbeauftragter) der Hauptniederlassung oder einzigen Niederlassung des Verantwortlichen)

d. Dokumentation gemäß Art. 33 Abs. 5 DS-GVO durchführen

- ☐ Beschreibung aller relevanten Fakten
- ☐ Auswirkungen der Datenschutzverletzung
- ☐ Ergriffene Maßnahmen

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

e. Mitarbeiter darauf hinweisen, dass sämtliche – auch vermeintlich „unerhebliche“ - Datenschutzverletzungen dem betrieblichen Datenschutzbeauftragten zu melden sind

f. Betrieblichen Datenschutzbeauftragten bei der Meldung an die Aufsichtsbehörde einbeziehen

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

1. Checkliste

Aus den vorstehenden Ausführungen ergibt sich folgende empfohlene Vorgehensweise in Form einer Checkliste:

a. Liegen Anhaltspunkte für eine Verletzung des Schutzes personenbezogener Daten vor?

☐ Angriff auf das Computersystem von außen, z. B. durch Viren oder Trojaner

☐ Verlust von Laptops, Smartphones, USB-Sticks, externen Festplatten oder Sicherungsbändern

☐ Diebstahl eines Smartphones oder eines IT Systems (PC, Notebook, Laptop, Tablet)

☐ unbefugtes Weitergeben von Daten durch Mitarbeiter

☐ unzulässige Nutzung personenbezogener Daten

☐ Einbruch in bzw. unbefugter Zutritt in Räumlichkeiten, in denen personenbezogene Daten aufbewahrt werden

☐ Sonstiges: _____

Ist das Ereignis:

☐ „Bekanntgeworden“ (tatsächliche Anhaltspunkte, hohe Wahrscheinlichkeit)

b. Besteht dadurch ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen?

☐ Erfordert Risikoabwägung (Prognose über mögliche Auswirkungen unter Berücksichtigung von Eintrittswahrscheinlichkeit und möglicher Schadensschwere)

Im Sozial und Gesundheitswesen ist grundsätzlich davon auszugehen, dass ein benachrichtigungspflichtiges Ereignis vorliegt, wenn personenbezogene Patientendaten unrechtmäßig an Dritte übermittelt wurden oder Dritte diese auf sonstige Weise unrechtmäßig zur Kenntnis nehmen konnten

- **Falls nein: Keine Informationspflicht gegenüber der betroffenen Person, aber Dokumentationspflicht gemäß Art. 34 Abs. 2 DS-GVO!**
- **Falls ja: Betroffene Person muss über Datenschutzverletzung informiert werden**

c. Inhalt der Meldung: siehe Art. 34 Abs. 2 DS-GVO

- ☐ Name und Kontaktdaten des betrieblichen Datenschutzbeauftragten
- ☐ wahrscheinliche Verletzungsfolgen
- ☐ ergriffene oder vorgeschlagene Maßnahmen
- ☐ Zeitpunkt: unverzüglich (beachte: anderer Maßstab als bei Meldung an Aufsichtsbehörde!)
  - es können je nach Einzelfall durchaus zunächst Sicherungsmaßnahmen getroffen werden; ggf. Benachrichtigungszeitpunkt mit Aufsichtsbehörde abstimmen
  - 72 Std: Frist sollte nach Möglichkeit eingehalten werden
- ☐ Form: in Textform, Klare und einfache Sprache

d. Ausnahmen von der Benachrichtigungspflicht sorgfältig prüfen (Art. 34 Abs. 3 DS-GVO, ggf. § 29 Abs. 1 Satz 3 und 4 BDSG neue Fassung[47]):

- ☐ Es wurden vorab geeignete Sicherheitsvorkehrungen gegen Datenschutzverletzungen getroffen (z. B. Verschlüsselung)
- ☐ nachträgliche Maßnahmen möglich, die die Risiken für betroffene Personen aller Wahrscheinlichkeit nach entfallen lassen? Z. B.:
  - Vertraulichkeitsvereinbarung mit dem unberechtigten Empfänger personenbezogener Daten
  - Individuelle Benachrichtigung mit unverhältnismäßigem Aufwand verbunden, z. B. weil zu großer Personenkreis?
    - Beachte: Dann aber Information auf anderem Wege erforderlich (öffentliche Bekanntmachung, z. B. Tageszeitung)

e. Aufsichtsbehörde kann bei unterbliebener Benachrichtigung vom Verantwortlichen verlangen, dies nachzuholen oder sie kann per Beschluss feststellen, dass Voraussetzungen für Benachrichtigungspflicht erfüllt sind (Art. 34 Abs. 4 DS-GVO)