Umgang mit Datenschutzverletzungen
Handlungsanweisung

Diese Handlungsanweisung soll den vom Unternehmen getroffenen Maßnahmen zum Umgang mit Datenschutzverletzungen nach Art. 33 und 34 DSGVO dienen.

1. Geltungsbereich

Diese Handlungsanweisung gilt für alle hauptamtlich Beschäftigten sowie jeglicher sonstigen vertraglich gebundenen Angestellten und Einsatzkräften der Jugendhilfe Essen gGmbH und der Jugendberufshilfe Essen gGmbH.

2. Definition von Datenschutzverletzungen

Eine Datenschutzverletzung ist ein Verstoß gegen die Datensicherheit und den Datenschutz, bei dem personenbezogene Daten Unberechtigten vermutlich oder erwiesenermaßen bekannt werden. Die Ursachen dafür sind vielfältig und können z.B. in einem Hackerangriff, dem Verlust eines USB-Sticks, dem Diebstahl eines Notebooks oder im unbefugten Weitergeben von Daten durch Mitarbeitende – gleich ob bewusst oder unbewusst – liegen.

3. Pflichten bei einer Datenschutzverletzung

- Der Arbeitgeber muss Verletzungen des Schutzes personenbezogener Daten, von denen mehr als nur ein geringes Risiko für die Rechte und Freiheiten natürlicher Personen ausgeht, der zuständigen Aufsichtsbehörde unverzüglich, möglichst binnen 72 Stunden, melden (Art. 33 DS-GVO).

- Neben der Meldung an die Aufsichtsbehörde sind im Falle des Art. 34 DS-GVO auch die betroffenen Personen unverzüglich zu informieren. Das ist dann der Fall, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat. Ob und welche Maßnahmen im Rahmen des Art. 33 Abs. 3 erfolgten, ist ebenfalls der Aufsichtsbehörde mitzuteilen.

- Es ist eine Beschreibung zu den technisch-organisatorischen Maßnahmen zur Beseitigung des Vorfalls sowie Maßnahmen zum Schutz der Betroffenen zu erstellen.

- Die Datenschutzpanne ist zu dokumentieren.

4. Interne Meldung

Die Feststellung einer Datenschutzverletzung (Verletzung des Schutzes personenbezogener Daten) ist gem. Art. 33 und 34 DSGVO **immer** und **umgehend** der Leitung des Zentralen Service und der jeweiligen Führungskraft zu melden. Die Meldung hat über den dafür vorgesehenen Meldebogen zu erfolgen. Dieser ist im Dokumentenmanagement unter dem Themenordner „Datenschutz“ abgelegt. Das gilt auch, wenn nur der Verdacht besteht, dass sich eine Datenschutzverletzung ereignet hat, der*die Mitarbeitende selbst dies aber nicht abschließend beurteilen kann. Dieser Bogen ist auch für Personen zu nutzen, die selber von einer Datenschutzverletzung betroffen sind und nicht nur eine solche festgestellt haben oder vermuten.

Die Leitung des Zentralen Service geht umgehend mit dem*der externen Datenschutzbeauftragten, der Führungskraft in den weiteren Austausch und Prüfung des Sachverhalts. Bei Bedarf werden hierzu weitere Personen, wie zum Beispiel die meldende Person, mit involviert. Der Meldebogen wird gemeinsam bei sich neu ergebenden Informationen, durch den zuvor genannten Personenkreis ergänzt oder angepasst. Die Geschäftsführung ist über den Sachverhalt zu informieren.

5. Benachrichtigung an die betroffene(n) Person(en)

Bedeutet die Datenschutzverletzung voraussichtlich ein “hohes Risiko” für die persönlichen Rechte und Freiheiten der von der Datenschutzverletzung betroffenen Person(en), werden die Betroffenen Personen unverzüglich über die Datenschutzverletzung benachrichtigt. Zwischen der Leitung Zentraler Service und Führungskraft wird entschieden, wer die betroffenen Personen informiert.

Ein hohes Risiko wird regelmäßig dann anzunehmen sein, wenn sich eine Prognose ergibt, dass mit hoher Wahrscheinlichkeit ein Schaden für die Rechte und Freiheiten der betroffenen Person eintritt (bspw. finanzielle Verluste/unberechtigte Abbuchungen, Identitätsbetrug oder Offenlegung privater Informationen). Maßgeblich ist hierbei auch, ob und inwieweit weitere Verletzungen durch die Benachrichtigung vermieden werden können.

Die Benachrichtigung muss in klarer und einfacher Sprache erfolgen. Der*Die Betroffene muss verstehen, was passiert ist, um einschätzen zu können, welche Risiken für ihn*sie durch das Ereignis bestehen und welche Maßnahmen er*sie ergreifen kann, um eventuell eintretende Schäden zu verhindern.

Die Benachrichtigung muss enthalten:

- eine Beschreibung der Art der Datenschutzverletzung,
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen,
- eine Beschreibung der wahrscheinlichen Folgen der Datenschutzverletzung; bspw. Identitätsmissbrauch (etwa bei Onlinegeschäften), Herbeiführung von Vermögensschäden (etwa durch unberechtigte Abbuchungen), Herbeiführung sozialer und/oder beruflicher Nachteile, Herbeiführung sonstiger Nachteile),
- eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung oder Abmilderung der Verletzung (Ursachenbeseitigung und Schadensbegrenzung); bspw. Änderung von Passwörtern und PIN-Codes, Kontrolle von Kontoauszügen auf Unregelmäßigkeiten; Kontrolle von Online-Konten auf Unregelmäßigkeit, Information von Kreditinstituten und Kreditkartengesellschaft.

Die Benachrichtigung der betroffenen Person ist nicht erforderlich, wenn:

- vor dem Vorfall technische und organisatorische Sicherheitsvorkehrungen (z.B. Verschlüsselung) getroffen wurden, durch die personenbezogene Daten für unbefugte Personen unzugänglich gemacht wurden,
- durch nachfolgende Maßnahmen sichergestellt wurde, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen aller Wahrscheinlichkeit nach nicht mehr besteht,

- die Benachrichtigung der betroffenen Personen mit einem unverhältnismäßigen Aufwand verbunden wäre, bspw. aufgrund der Vielzahl der Fälle. Stattdessen erfolgt eine öffentliche Bekanntmachung (z. B. durch Anzeigen, die mindestens eine halbe Seite umfassen, in mindestens zwei lokal erscheinenden Tageszeitungen) oder eine ähnliche Maßnahme, durch die die betroffenen Personen vergleichbar wirksam informiert werden (bspw. Nutzung elektronischer Medien oder Verwendung regionaler Zeitungen, wenn der Kreis der Betroffenen entsprechend lokal angesiedelt ist).

Verantwortlich ist die Leitung des Zentralen Service, bzw. die von der Geschäftsführung beauftragte Person. Der Datenschutzbeauftragte steht beratend zur Verfügung.

6. Meldung an die Aufsichtsbehörde

Für Meldungen an die Aufsichtsbehörde ist das Formular zu verwenden, welches über folgenden Link zu finden ist:

https://www.ldi.nrw.de/kontakt/meldeformular-fuer-datenpannen

Zwischen der Leitung des Zentralen Service und dem*der externen Datenschutzbeauftragten wird festgelegt, wer die Meldung der Datenschutzverletzung durchführt.

7. Dokumentation des Vorfalls

Jede Datenschutzverletzung muss gem. Art. 33 und 34 DSGVO dokumentiert werden. Den Behörden soll damit ermöglicht werden, bei einer Betriebsprüfung zu kontrollieren, ob u. a. die Benachrichtigungspflichten eingehalten wurden. Die Dokumentation ist im Dokumentenmanagement der Geschäftsführung abzulegen.

Verantwortlich ist der Datenschutzbeauftragte, die Führungskraft oder dessen Vertreter*in, je nachdem, wer die Dokumentation durchführt.

8. Veröffentlichung der Handlungsanweisung

Die Handlungsanweisung wird im Dokumentenmanagement veröffentlicht und regelmäßig auf Aktualität geprüft.

Essen, den 17.06.2024

ppa.

Leitung Zentraler Service