Wenn es passiert ist:
Meldungen von Datenpannen

Sommerakademie
am 12. September 2022
in Kiel

Maren Nielsen / Alexander Hauptmann
0431 988-1651/1283
ULD45/46@datenschutzzentrum.de
https://www.datenschutzzentrum.de/

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Ablauf

1. Wann (unter welchen Voraussetzungen) muss eine Meldung nach Art. 33 DSGVO erfolgen?
2. Wie erfolgt eine Meldung nach Art. 33 DSGVO ?
3. Weitere Bearbeitung des ULD nach Eingang der Meldung
4. Zusammenfassung/Abschluss

1. Wann muss eine Meldung nach Art. 33 DSGVO erfolgen?

Art. 33 Abs. 1 DSGVO

Im Falle einer Verletzung des Schutzes personenbezogener Daten

meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde,

es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führt.

ULD www.datenschutzzentrum.de

1. Wann muss eine Meldung nach Art. 33 DSGVO erfolgen?

Verletzung des Schutzes personenbezogener Daten
> Begriffsbestimmung gem. Art. 4 Nr. 12 DSGVO

Der Ausdruck „Verletzung des Schutzes personenbezogener Daten" bezeichnet eine **Verletzung der Sicherheit**, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden

1. Wann muss eine Meldung nach Art. 33 DSGVO erfolgen?

Art. 4 Nr. 12 DSGVO Verletzung der Sicherheit
> Art. 32 DSGVO Sicherheit der Verarbeitung

Art. 32 Abs. 1 DSGVO: Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

1. Wann muss eine Meldung nach Art. 33 DSGVO erfolgen?

Art. 33 Abs. 1 DSGVO

Im Falle einer Verletzung des Schutzes personenbezogener Daten

meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde,

es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führt.

1. Wann muss eine Meldung nach Art. 33 DSGVO erfolgen?

Risiko gem. ErwGr. 75 und 95 Satz 2 DSGVO

Ein Risiko im Sinne der DSGVO ist das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann.

Es hat zwei Dimensionen: Erstens die **Schwere des Schadens** und zweitens die **Wahrscheinlichkeit, dass das Ereignis und die (Folge-)Schäden eintreten**.

1. Wann muss eine Meldung nach Art. 33 DSGVO erfolgen?

Schaden – physisch, materiell oder immateriell

- finanzieller Verlust
- wirtschaftliche Nachteile
- Identitätsdiebstahl
- gesellschaftliche Nachteile
- Rufschädigung
- körperliche Schäden
- Diskriminierung

1. Wann muss eine Meldung nach Art. 33 DSGVO erfolgen?

Eintrittswahrscheinlichkeit

Die Eintrittswahrscheinlichkeit eines Risikos beschreibt, mit welcher Wahrscheinlichkeit ein bestimmtes Ereignis (das selbst auch ein Schaden sein kann) eintritt und mit welcher Wahrscheinlichkeit es zu Folgeschäden kommen kann.

1. Wann muss eine Meldung nach Art. 33 DSGVO erfolgen?

Art. 33 Abs. 1 DSGVO

Im Falle einer Verletzung des Schutzes personenbezogener Daten

meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde,

es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führt.

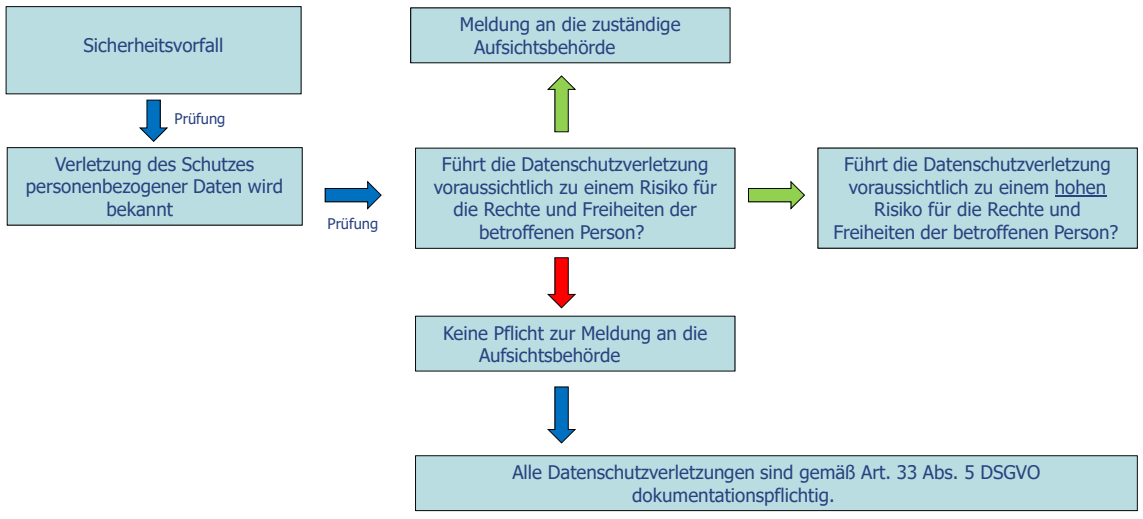
1. Wann muss eine Meldung nach Art. 33 DSGVO erfolgen?

Verletzung des Schutzes personenbezogener Daten

Der Ausdruck „Verletzung des Schutzes personenbezogener Daten" bezeichnet eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden

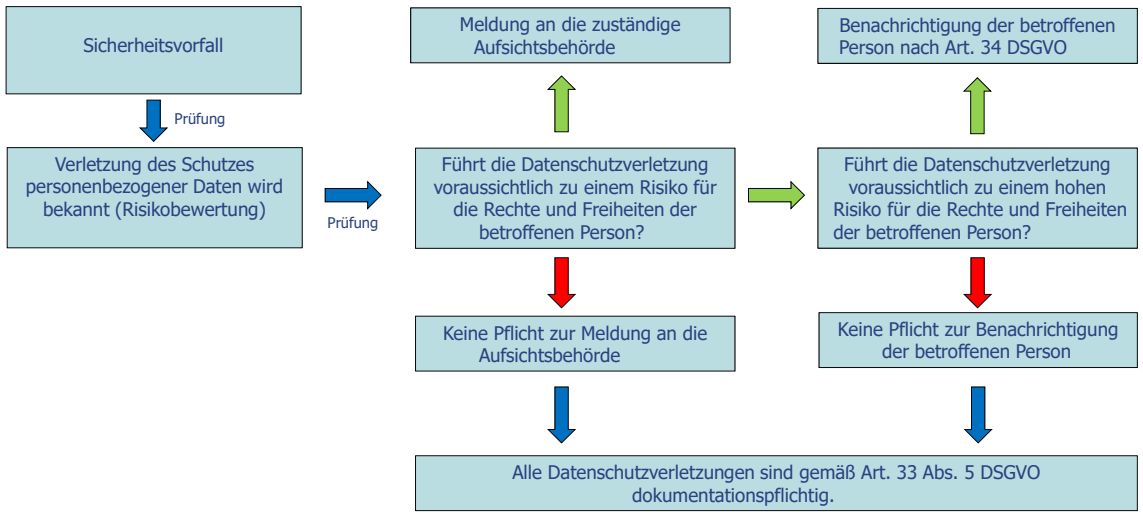
! ! !

Ablauf einer Meldung nach Art. 33 DSGVO



Pflicht zur Benachrichtigung gem. Art. 34 Abs. 1 Buchst. d DSGVO

Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.



2. Wie erfolgt die Meldung nach Art. 33 DSGVO?

Gem. Art. 33 Abs. 3 DSGVO enthält die Meldung zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze

b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen

ULD www.datenschutzzentrum.de

2. Wie erfolgt die Meldung nach Art. 33 DSGVO?

Gem. Art. 33 Abs. 3 DSGVO enthält die Meldung zumindest folgende Informationen:

c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten

d) eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

3. Was passiert mit den Meldungen gem. Art. 33 DSGVO?

Die Aufsichtsbehörde muss in ihrem Hoheitsgebiet die Anwendung der DSGVO überwachen und durchsetzen (Art. 57 Abs. 1 Buchst. a DSGVO)

- Prüfung, ob die Meldung den Vorgaben des Art. 33 DSGVO entspricht
- Prüfung, ob die personenbezogenen Daten zum Zeitpunkt des Vorfalls in einer Weise verarbeitet wurden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistete (Art. 5 Abs. 1 Buchst. f DSGVO i.V.m. Art. 32 DSGVO).

3. Was passiert mit den Meldungen gem. Art. 33 DSGVO?

Sicherheit der Verarbeitung gem. Art. 32 Abs. 1 Buchst. d DSGVO

Die durch den Verantwortlichen zu treffenden technischen und organisatorischen Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, schließen unter anderem Folgendes ein:

- Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

> Welche Maßnahmen wurden ergriffen, um einen erneuten gleichartigen Vorfall zu verhindern?

3. Was passiert mit den Meldungen gem. Art. 33 DSGVO?

Entscheidung über Untersuchungs- oder Abhilfebefugnisse gem. Art. 58 DSGVO durch die Aufsichtsbehörde

z.B.

- Hinweis gem. Art. 58 Abs. 1 Buchst. d DSGVO bei einem vermeintlichen Verstoß gegen die Datenschutz-Grundverordnung

- Verwarnung gem. Art. 58 Abs. 2 Buchst. b, wenn der Verantwortliche mit Verarbeitungsvorgängen gegen diese Verordnung verstoßen hat

Zusammenfassung

1. Wann (unter welchen Voraussetzungen) muss eine Meldung nach Art. 33 DSGVO erfolgen?
2. Wie erfolgt eine Meldung nach Art. 33 DSGVO, und was ist Inhalt der Meldung?
3. Was passiert nach Abgabe der Meldung?
4. Relevanz der Prüfung, ob eine Verletzung des Schutzes personenbezogener Daten vorliegt und ob diese Verletzung zu einem hohen Risiko für die Rechte und Freiheiten der betroffenen Personen führt
5. Anforderungen der Aufsichtsbehörde an die Meldung nach Art. 33 DSGVO

Vertiefende Literatur

- Art. 29-Datenschutzgruppe, Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679, WP250rev.01, 2018, https://ec.europa.eu/newsroom/article29/items/612052
- Kurzpapier Nr. 18 der DSK „Risiko für die Rechte und Freiheiten natürlicher Personen“, https://www.datenschutzzentrum.de/artikel/1225-.html
- EDPB Guidelines 01/2021 on Examples regarding Data Breach Notification, 2021, https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012021_pdbnotification_adopted_en.pdf
- Webseite des ULD: www.datenschutzzentrum.de