 

  DFN-CERT Services GmbH Logo

Handreichung zur Benachrichtigung Betroffener bei Datenschutzvorfällen gemäß Art. 34:

**Checkliste für Verantwortliche zur Formulierung des Informationstextes**

Version 2.0, 3. Mai 2019

Die Nutzung dieses Dokuments ist zulässig unter der Lizenz CC BY-SA 3.0     
<https://creativecommons.org/licenses/by-sa/3.0/de/legalcode>

Autor: NRW Projektgruppe „Umsetzung der EU-Datenschutz-Grundverordnung (EU-DSGVO) −   
Datenschutzmanagementsysteme“ 2018

gefördert vom 

**Worum geht es?**

Bei IT-Sicherheitsvorfällen, die auch personenbezogene Daten betreffen, besteht gem. Art. 33 DS-GVO für die Verantwortliche bzw. den Verantwortlichen (Präsidentin/Präsident bzw. Rektorin/Rektor der Hochschule) eine Meldepflicht des Vorfalls innerhalb von 72 Stunden ab Kenntnisnahme des Vorfalls durch die Hochschule an die Datenschutz-Aufsichtsbehörde (LDI NRW).

Die Meldung wird durch ein „Einsatzteam“ unter Beteiligung der/des Datenschutzbeauftragten und der/des IT-Sicherheitsbeauftragten für die/den Verantwortliche/n vorbereitet.

Ergibt die Prüfung durch das Einsatzteam, dass die mit dem Sicherheitsvorfall verbundene Datenschutzverletzung **voraussichtlich ein hohes Risiko** für die betroffenen Personen zur Folge hat, so **benachrichtigt** die Hochschule als Verantwortliche die betroffene/n Person/en unverzüglich von der Verletzung. (vgl. Art. 34 DS-GVO).

Die Meldung über den Vorfall an den LDI NRW ist, nach Vorbereitung durch das „Einsatzteam“ von/vom der/dem Präsident/in bzw. Rektor/in durchzuführen bzw. durchführen zu lassen. Die/der operativ Verantwortliche wird jeweils vom „Einsatzteam“ hinzugezogen. Die Information der betroffenen Personen gem. Art. 34 DS-GVO ist i. d. R. unverzüglich von dem/der operativ Verantwortlichen durchzuführen.

Wenn die Betroffenen über einen Datenschutzvorfall informiert werden (z.B. weil dies nach Art. 34 DS-GVO notwendig ist), so muss über diese Information an Betroffene auch der LDI NRW im Rahmen der Meldung von geplanten, bzw. schon getroffenen Maßnahmen informiert werden (Art. 33 (3) d) DS-GVO).

**Wie ist diese Checkliste einzusetzen?**

Die Checkliste soll das „Einsatzteam“ und die/den operativ Verantwortliche/n dabei unterstützen, den Text einer Information von betroffenen Personen rechtskonform und vollständig zu formulieren bzw. dies zu prüfen und zu dokumentieren.

# Checkliste zur Formulierung eines Informationstextes für Betroffene von Vorfällen gem. Art. 34 i. V. m. Art. 33 Abs. 3, lit. b, c und d DS-GVO.

Vorfall, Datum des Vorfalls:

Operativ Verantwortliche/r:

ggf. Beabeiter/in:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Werden die folgenden Punkte im Informationstext hinreichend beschrieben? | **Fundstelle** | **Erläuterung** |  | Anmerkungen |
| Mindestens erforderliche Inhalte der Information | | | | |
| Beschreibung der Verletzung in klarer und einfacher Sprache (insbesondere das Vorliegen einer Vernichtung, des Verlusts, einer Veränderung und/oder einer unbefugten Offenlegung von (bzw. zum Zugang zu) personenbezogenen Daten) | Art. 34 Abs.2 S. 1 | Die Verletzung des Schutzes personenbezogene Daten ist präzise und transparent, zugleich in für Laien einfach verständlicher Sprache zu formulieren. | enthalten |  |
| Name und Kontaktdaten der/des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Information | Art. 33 Abs. 3 lit. b | Hier ist immer die Stelle anzugeben, die jeweils am besten fachlich geeignet ist, über den konkreten Vorfall informiert und kompetent Auskunft zu geben.[[1]](#footnote-1) | enthalten |  |
| Eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten (z.B. Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, Rufschädigung, Verlust der Vertraulichkeit oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile) | Art. 33 Abs. 3 lit. c | Schutzperspektive beachten: Gemeint sind nachteilige Folgen für die Betroffenen, nicht für die Institution. | enthalten |  |
| Eine Beschreibung der von der verantwortlichen Hochschule ergriffenen oder geplanten Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten | Art. 33 Abs. 3 lit. d |  | enthalten |  |
| Ggf. eine Beschreibung der von der verantwortlichen Hochschule ergriffenen oder geplanten Maßnahmen zur Abmilderung der möglichen nachteiligen Auswirkungen der Verletzung | Art. 33 Abs. 3 lit. d | Wird „nicht erforderlich“ ausgewählt, muss die fehlende Erforderlichkeit begründet werden, z.B.:  Es gibt keine denkbare oder praktisch umsetzbare Maßnahme zur Abmilderung.  Das Risiko konnte durch Maßnahmen bereits ausgeschlossen werden. | enthalten nicht erforderlich | Begründung im Falle von „nicht erforderlich“ bitte hier formulieren: |

1. Dazu Paal/Pauly Art. 33 Rn.48: „Es kann aber in Einzelfällen dennoch sinnstiftend sein, eine andere Stelle [als den/die DSB] in der Meldung anzugeben, etwa weil diese bereits über eine ***bessere Informationslage oder aber weiterreichende Entscheidungsbefugnisse verfügt*** (vgl. Sassenberg in Sydow DS-GVO Art. 33 Rn. 20“ [↑](#footnote-ref-1)