Muster: Rundschreiben an alle Beschäftigten zur Meldung von Datenschutzverletzungen

(Stand 20.05.2019)

(anzupassende Stellen sind rot markiert)

Meldung von Informationssicherheitsvorfällen / Datenschutzverletzungen

Sehr geehrte Damen und Herren,

innerhalb der Hochschule wird in allen Bereichen (Zentralverwaltung, Fakultäten/Fachbereichen, Institute/Departments, Zentrale Einrichtungen …) mit personenbezogenen Daten gearbeitet. Das können Namen, Adressen, Verträge, Forschungsdaten oder Klausurergebnisse sein. Bei der Verarbeitung sind die datenschutzrechtlichen Regelungen einzuhalten, unter anderem die neuen Meldepflichten der Europäischen Datenschutzgrundverordnung (DS-GVO), die seit Mai 2018 gilt.

Falls es zu einer „Verletzung des Schutzes personenbezogener Daten“ (im Folgenden Datenschutzverletzung genannt) kommt, ist die Hochschule verpflichtet, diese binnen 72 Stunden der Aufsichtsbehörde zu melden, sofern Risiken für die Betroffenen nicht ausgeschlossen werden können.[[1]](#footnote-1)

Datenschutzverletzungen sind Verletzungen der Datensicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung personenbezogener Daten führen bzw. diese gegenüber Unbefugten offenlegen oder einen unbefugten Zugang zu personenbezogenen Daten ermöglichen.[[2]](#footnote-2)

Damit verbunden sind in den meisten Fällen Angriffe auf die IT-Systeme oder der unerlaubte Umgang mit personenbezogenen bzw. sensiblen Daten (Informationssicherheitsvorfälle). Sämtliche Angriffe, unerlaubte Datennutzung oder diesbezügliche Verdachtsmomente müssen sorgfältig geprüft werden, um Datenschutzverletzungen zu erkennen. Hierunter fallen beispielsweise

* Angriffe auf zentrale IT-Systeme (bspw. Campusmanagementsystem, Personalverwaltung, Lernplattform) oder dezentrale IT-Systeme (bspw. Umfragesysteme, Forschungsdatenbanken), bei denen Angreifer personenbezogene Daten zur Kenntnis gelangt sein können,
* Systemveränderungen oder Ausspähen von Zugangskennungen (Passwörter) durch massenhafte Verbreitung von Viren, Malware und Spam-Mails,
* die unbeabsichtigte Fehlkonfiguration eines Systems, sodass personenbezogene Daten ungewollt veröffentlicht werden,
* der versehentliche Versand personenbezogener Daten an einen für diese Daten nicht zuständigen E-Mail-Verteiler,
* der Verlust eines mobilen Endgeräts (Notebook, Smartphone) oder Datenträgers (USB-Stick), auf dem sich personenbezogene Daten befinden,
* aber auch die unzulässige Veröffentlichung papierbasierter Unterlagen wie namentliche Aushänge von Klausurergebnissen.

Damit die Hochschule ihrer Meldepflicht innerhalb der gesetzlichen Frist nachkommen kann, ist sie darauf angewiesen, von ihren Beschäftigten verlässlich und unmittelbar nach Bekanntwerden über sämtliche Informationssicherheitsvorfälle informiert zu werden.

Die Meldung erkannter Informationssicherheitsvorfälle durch Beschäftigte kann nur unterlassen werden, wenn sicher bekannt ist, dass der Vorfall bereits von anderen Beschäftigten der Hochschule gemeldet worden ist. Im Zweifel muss immer eine Meldung erfolgen. Der Meldeprozess hat dabei Vorrang vor dem allgemeinen Tagesgeschäft.

Sollte es zu einem vermeintlichen oder tatsächlichen Informationssicherheitsvorfall gekommen sein, ziehen Sie − soweit zeitnah verfügbar − die Leitung und die Datenschutzkoordinatorin / den Datenschutzkoordinator Ihres Bereichs und − wenn erforderlich − Kolleginnen, Kollegen, Administratorinnen oder Administratoren vor der Meldung hinzu. Unabhängig von der Meldung müssen Maßnahmen ergriffen werden, um die Datenschutzverletzung zu beheben oder mögliche Auswirkungen abzumildern.

Weitere Informationen finden Sie unter

<Link>

Füllen Sie bitte, soweit die erfragten Angaben bereits bekannt sind, das Meldeformular unter dem folgenden Link aus:

<Link>

Senden Sie das ausgefüllte Formular per E-Mail an die Adresse <vorfall@hochschule-X.de>.

Die abgegebenen Meldungen werden von einem „Vorfallteam“ bearbeitet. Dies besteht aus der/dem Datenschutzbeauftragten, der/dem Informationssicherheitsbeauftragten, der/dem CIO und … Dort wird der Vorfall geprüft und bewertet, wozu ggf. Rückfragen an die meldende Person oder die Organisationseinheit erfolgen und die Leitung der Organisationseinheit kontaktiert oder eingeladen wird. Ebenso können bei Bedarf weitere Personen (bspw. Administratorinnen oder Administratoren, die Systemdetails kennen oder Sicherheitsexpertinnen oder -experten von außerhalb der Hochschule) hinzugezogen werden. Der Name der meldenden Person wird auf Wunsch vom Vorfallteam vertraulich behandelt.

Bestehen mögliche Risiken für die Betroffenen, so wird der Vorfall schnellstmöglich der Aufsichtsbehörde, d. h. der Landesbeauftragten für Datenschutz und Informationsfreiheit NRW, gemeldet und ggf. werden die betroffenen Personen über die Datenschutzverletzung informiert. In jedem Falle werden der Vorfall und die Entscheidung dokumentiert und die betroffene Organisationseinheit sowie die Hochschulleitung erhalten entsprechende Informationen über den Vorfall.

Ich bitte um Beachtung und Bekanntgabe in Ihrem Bereich.

**Meldeprozess Informationssicherheitsvorfall**:

1. E-Mails an <vorfall@hochschule-X.de> werden in einem Ticketsystem verwaltet, das eine verlässliche und organisierte Abarbeitung sämtlicher Vorfälle unterstützt und von einem Vorfallteam bearbeitet, das aus DSB, IT-Sicherheitsbeauftragten, CIO und … besteht.
2. Im Vorfallteam wird der Vorfall geprüft und bewertet.

Ggf. werden weitere Informationen eingeholt, d. h. es erfolgen Rückfragen an die meldende Person oder die Organisationseinheit und die Leitung der Organisationseinheit wird kontaktiert oder eingeladen.

* 1. Bewertung, ob es sich um eine meldepflichtige Datenschutzverletzung im Sinne des Artikels 33 DS-GVO oder um eine Datensicherheitsverletzung handelt.
	2. Bewertung, ob die Betroffenen im Sinne des Artikels 34 DS-GVO informiert werden müssen.
	3. Sofern es sich um eine Datensicherheitsverletzung handelt, wird ein gesonderter Prozess in Gang gesetzt.
	4. Ergreifen von Sofortmaßnahmen in Abstimmung mit den betroffenen Bereichen innerhalb der Hochschule.
1. Bericht an das Präsidium bzw. an die Vizepräsidentin für Wirtschafts- und Personalverwaltung.
2. Ggf. Meldung an die Aufsichtsbehörde und Informieren der Betroffenen (bei Datenschutzverletzungen).
3. Dokumentation des Vorfalls (auch bei Nicht-Meldung an die Aufsichtsbehörde bzw. Präsidium).
4. Rückmeldung an die Leitung der Organisationseinheit und/oder den/die Vorfallmelder/in.
1. Vgl. Art. 33 DS-GVO [↑](#footnote-ref-1)
2. Vgl. Art. 4 Nr. 12 DS-GVO [↑](#footnote-ref-2)