Richtlinie

Behandlung von Informationssicherheits- und Datenschutzvorfällen an der Hochschule Hannover (Melderichtlinie)

1. Einleitung

Im Rahmen des Datenschutzes und der Informationssicherheit ist die Kenntnisnahme von Vorfällen und schnelle Reaktion ein wichtiger Bestandteil eines Sicherheitskonzeptes. Die Beeinträchtigung der Vertraulichkeit, Integrität und Verfügbarkeit stellen Vorfälle dar, die es durch geeignete Vorkehrungen zu unterbinden gilt, die aber nie gänzlich ausgeschlossen werden können.

2. Geltungsbereich

Die Richtlinie legt Maßnahmen im Umgang mit Informationssicherheitsvorfällen und Verletzungen des Schutzes personenbezogener Daten fest, um Personen und Werte angemessen zu schützen. Mit Anwendung der Richtlinie werden die Anforderungen der Datenschutzgrundverordnung (DSGVO) nach Art. 33 Verletzung des Schutzes personenbezogener Daten umgesetzt.

3. Definition

Ein Informationssicherheitsvorfall (IS-Vorfall) zeichnet sich durch den Verlust oder absehbaren Verlust mindestens eines der Schutzziele Verfügbarkeit, Integrität, Vertraulichkeit und Belastbarkeit aus.

Eine Verletzung des Schutzes personenbezogener Daten ist in Art. 4 Nr. 12 DSGVO definiert als 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.

Die Verletzung des Schutzes personenbezogener Daten ist im Sinne dieser Richtlinie auch immer ein IS-Vorfall.

Zur Bestimmung des Risikos ist das Schadenspotential in Beziehung zur Eintrittswahrscheinlichkeit zu setzen.

Die vorliegende Richtlinie unterscheidet zwei Abstufungen von IS-Vorfällen. Ein IS-Vorfall liegt vor, falls

- eine Verletzung personenbezogener Daten vorliegt, dieser Vorfall aber voraussichtlich kein Risiko für die Rechte und Freiheiten natürlicher Personen darstellt,
- die Funktionsfähigkeit der Hochschule in Teilen beeinträchtigt ist,
- der Ruf der Hochschule in Mitleidenschaft gezogen wird,

- der IS-Vorfall negative Auswirkungen auf Personen oder Systeme außerhalb der Hochschule haben kann, oder
- hochschulweite Richtlinien mit Bezug zur Informationsverarbeitung verletzt werden.

Ein schwerwiegender IS-Vorfall liegt vor

- falls eine Verletzung personenbezogener Daten voraussichtlich ein Risiko für die Rechte und Freiheiten natürlicher Personen nach DSGVO Art. 33 darstellt,
- wenn der IS-Vorfall sich auf besondere personenbezogene Daten nach DSGVO Art. 9 bezieht,
- bei Gefährdung eines Schutzzieles mit einem finanziellen Schadensumfang für die Hochschule von über 50.000€,
- wenn der Ruf der Hochschule in besonderem Maße beeinträchtigt wird,
- wenn die Funktionsfähigkeit der Hochschule länger als zwei Werktage schwerwiegend beeinträchtigt ist,
- der IS-Vorfall in hohem Maße negative Auswirkungen auf Personen oder Systeme außerhalb der Hochschule haben kann, oder
- bei Verletzung von Gesetzen und Verordnungen in Bezug zur Informationsverarbeitung.

4. Festlegung der Verantwortung

Federführend für die Erstellung, Inkraftsetzung und Überprüfung der Richtlinie und Entscheidung bei Vorfällen auf Präsidiumsebene ist der für das Ressort IT zuständige Vizepräsident / die Vizepräsidentin, vertreten durch den / die Präsidenten / Präsidentin, den / die Hauptberufliche Vizepräsident / Vizepräsidentin oder die Leitung des Dezernats I - Personal und Recht.

Die Verantwortung für die Umsetzung des Informationssicherheitsprozesses laut Richtlinie trägt der Informationssicherheitsbeauftragte vertreten durch die Leitung der Hochschul-IT.

Verantwortlich für die Umsetzung der Richtlinie in den Fakultäten ist der/die Dekan*in, in Instituten die Institutsleitung.

In der Verwaltung, den Stabsstellen und den Einrichtungen sind die Leitungen der Organisationsein- heiten für die Umsetzung der Richtlinie verantwortlich.

Die Verantwortung für ein Verfahren und die damit verbundenen Daten liegt bei der Organisationseinheit, die laut Geschäftsverteilungsplan das Verfahren betreut.

Einzelne oder mehrere Abläufe dieser Richtlinie können durch die Verantwortlichen an Organisati-onseinheiten innerhalb der Hochschule delegiert werden. Die Verantwortung für die Umsetzung der Richtlinie verbleibt beim Verantwortlichen. Die Delegation hat schriftlich zu erfolgen und ist in Kopie dem Informationssicherheitsbeauftragten zuzuleiten. Die Delegation an Externe bedarf der Genehmigung durch das Präsidium.

5. Sanktionen

Die Nichteinhaltung der Richtlinie ist ein Verstoß gegen die Benutzungsordnung für die Informationsverarbeitungssysteme der Fachhochschule Hannover (IVS-BO) und kann nach §6 der IVS-BO geahndet werden.

6. Planung

Die Verantwortlichen müssen bereits bei der Planung des Einsatzes von informationsverarbeitenden Verfahren und Systemen das Auftreten von möglichen IS-Vorfällen unter expliziter Betrachtung der damit verbundenen Risiken berücksichtigen.

Vor Einsatz ist sicherzustellen, dass

- eine Einschätzung der Risiken mit Eintrittswahrscheinlichkeiten und potentiellen Schäden an im Vorfeld festgelegten Kriterien erfolgt,
- Maßnahmen zur Verhinderung, Erkennung und Behandlung von IS-Vorfällen den mit dem Verfahren verbundenen Risiken entsprechen ausgewählt wurden,
- schwerwiegende IS-Vorfälle erkannt werden,
- die unten festgelegten Informationen zu einem eingetretenen IS-Vorfall in den festgelegten Fristen weitergeleitet wird,
- Handlungsoptionen und Zuständigkeiten im Zusammenhang mit dem Umgang mit IS-Vorfällen festgelegt und bekannt sind,
- externe Parteien vertraglich zur Einhaltung verpflichtet sind,
- eine Überprüfung der Wirksamkeit und Anpassung der getroffenen Maßnahmen im jährlichen Turnus erfolgt,
- die Dokumentation einer Verletzung des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen (DSGVO Art 33 Abs. 5) gewährleistet ist,
- eine Dokumentation angelehnt an anerkannte Standards zur Informationssicherheit geführt wird, und
- die notwendigen Ressourcen, insbesondere qualifiziertes Personal, zur Umsetzung zur Verfügung stehen.

7. Erkennen von IS-Vorfällen

Der Verantwortliche stellt sicher, dass IS-Vorfälle zeitnah erkannt werden. Die dafür erforderlichen Erkennungsmaßnahmen wahren die Verhältnismäßigkeit in Bezug auf

- die Effektivität und dem dafür erforderlichem Aufwand in der Erkennung von Sicherheitsvorfällen,
- den Stand der Technik,
- dem Risiko,
- den Eingriff in die Rechte von Personen, die durch die Erkennungsmaßnahmen betroffen sind.

Die Überwachung der Maßnahmen hat so zu erfolgen, dass

- die Auswertung der Maßnahmen im Rahmen der Löschfrist erfolgt und eine Verfolgung der IS-Vorfälle möglich ist,
- die Kontrolldichte dem Risiko- und Schadenspotential angemessen ist,
- Fristen von Gesetzen und Verordnungen eingehalten werden können.

Personenbezogene Daten, die im Rahmen der Erkennung erhoben werden, sind nach 10 Werktagen zu löschen. In begründeten Verdachtsfällen ist eine längerfristige Speicherung zulässig. Eine Überprüfung der Zulässigkeit hat mindestens nach drei Monaten zu erfolgen. Ausnahmen von der Löschung sind zu dokumentieren.

8. Meldung von IS-Vorfällen an interne Stellen

IS-Vorfälle sind durch die den Vorfall feststellenden Person generell und sofort bei Bekanntwerden der für das jeweilige informationsverarbeitende Verfahren verantwortlichen Stelle zu melden. Im Zweifel wird der Vorfall dem IT-Service-Desk gemeldet unter

Mail support-it@hs-hannover.de Telefon -1441

Der IT-Service-Desk informiert in diesem Fall sofort die für das jeweilige informationsverarbeitende Verfahren verantwortlichen Stelle.

Die Einschätzung, ob ein schwerwiegender IS-Vorfall vorliegt, erfolgt dann durch den Verantwortlichen des betroffenen Verfahren. Im Zweifelsfall ist der Informationssicherheitsbeauftragte in die Bewertung einzubeziehen. Die Wahrung der Fristen hat zu erfolgen.

Schwerwiegende IS-Vorfälle sind durch den Verantwortlichen des betroffenen Verfahrens unverzüglich nach Bekanntwerden, spätestens am nächsten Tag 12.00 Uhr beim Informationssicherheitsbeauftragten zu melden. Fällt der nächste Tag auf einen arbeitsfreien Tag (Samstag, Sonntag oder Feiertag) so erfolgt die Meldung noch am Tage des Bekanntwerdens. Die Meldung gilt nach Bestätigung des Eingangs durch den Informationssicherheitsbeauftragten als erfolgt. Nicht schwerwiegende IS-Vorfälle werden analog gemeldet, jedoch gilt hierfür eine Frist von 5 Werktagen.

Wenn und soweit die Informationen nicht zum Zeitpunkt der ersten Bekanntgabe bereitgestellt werden können, kann der Verantwortliche diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.

Die Meldung enthält

- den Verantwortlichen des Verfahrens mit Kontaktdaten,
- eine Beschreibung des aufgetretenen Vorfalls,
- eine Abschätzung des Schadens,
- die zu erwartenden oder festgestellten Auswirkungen auf Schutzziele, und
- unternommene oder geplante Korrekturmaßnahmen mit Zeitplan.

Bei personenbezogenen Daten sind zusätzlich anzugeben oder zu präzisieren:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe

  der Kategorien (z.B. Beschäftige, Studierende) und der ungefähren Zahl der betroffenen Personen,

  der betroffenen Datenkategorien (z.B. Adressdaten, Kontodaten) und

  der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- 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.
- nähere Angaben ob und wenn ja wie, wann und durch wen die Benachrichtigung der Betroffenen erfolgen soll.

Die Mailadresse zur Meldung von IT-Vorfällen an den IT-Sicherheitsbeauftragten durch den Verantwortlichen des betroffenen Verfahrens ist it-sicherheit@hs-hannover.de oder hilfsweise der IT-Service-Desk unter 0511-9296-1441.

Die Meldung von IS-Vorfällen als schwerwiegende IS-Vorfälle ist unschädlich.

9. Meldung von IS-Vorfällen an externe Stellen

Externe Stellen sind Aufsichts- und Strafverfolgungsbehörden, andere öffentliche Stellen oder Verbände. Die Meldung an externe Stellen und die Kommunikation mit den Stellen erfolgt ausschließlich durch die Hochschulleitung oder eine von ihr beauftragte Stelle.

10. Reaktion auf IS-Vorfälle

Die Reaktion auf einen IS-Vorfall wird durch den Informationssicherheitsbeauftragten koordiniert. Dazu kann ein Team gebildet werden, bestehend aus

- dem verantwortlichen Präsidiumsmitglied
- dem / der Informationssicherheitsbeauftragten
- dem Leiter oder der Leiterin der betroffenen Organisationseinheit oder Fakultät

Die Teamleitung hat das verantwortliche Präsidiumsmitglied, im Verhinderungsfall vertreten durch den Informationssicherheitsbeauftragten. Sie kann zusätzliche Mitglieder anlassbezogen benennen. Im Regelfall sind dies

- Dezernat I - Personal und Recht
- OeM
- Hochschul-IT oder dezentrale IT-Abteilung

Mit Bekanntwerden eines schwerwiegenden IS-Vorfalls ist in jedem Fall ein Team zu bilden. Der/Die Datenschutzbeauftragte ist hierüber zu informieren und in die Bearbeitung einzubinden.

Die Mitarbeit im Team ist für die benannten Mitglieder verpflichtend.

Anweisungen des Teams zur Behebung des IS-Vorfalls und zur Abwehr von Schäden an Personen und Werten sind zu befolgen.

Der Datenschutzbeauftragte erhält in regelmäßigen Abständen, mindestens halbjährlich, eine Aufstellung über die aufgetretenen IS-Vorfälle durch den IT-Sicherheitsbeauftragten.

11. Überprüfung der Richtlinie

Eine Überprüfung der Richtlinie erfolgt mindestens jährlich im Rahmen einer Sitzung des IT- Strategieausschusses.

Die im Präsidium verantwortliche Stelle, stellt durch regelmäßige Überprüfungen die Einhaltung der Richtlinie sicher. Dazu kann sie interne wie externe Stellen beauftragen.

12. Zweckbindung und Vertraulichkeit des Verfahrens

Die Natur eines IS-Vorfalls führt in aller Regel zur Verarbeitung personen- oder schützenswerter Daten. Die Verarbeitung von personenbezogenen Daten erfolgt ausschließlich zum Zwecke der Erkennung, Bearbeitung und Behebung eines IS-Vorfalles. Eine anderweitige Nutzung ist unzulässig. Grundlage der Verarbeitung im Rahmen von IT-Systemen ist die Benutzungsordnung für die Informationsverarbeitungssysteme der Fachhochschule Hannover (IVS-BO) §7 vom 27.7.2005.

Bei der Verarbeitung ist die Vertraulichkeit zu wahren. Bei der Bearbeitung von IS-Vorfällen ist auf einen Personenbezug, soweit wie möglich, zu verzichten. Die Weitergabe von personenbezogenen Daten erfolgt ausschließlich im Rahmen der gesetzlich vorgeschriebenen Regelungen.

IS-Vorfälle werden 15 Jahre im Rahmen der Aktenführung aufbewahrt. Die Akte führt der Informationssicherheitsbeauftragte.

13. Ausnahmeregelung

Können Abläufe der Richtlinie nicht eingehalten werden, so ist unverzüglich das Präsidium zu informieren.

14. Inkrafttreten

Die Richtlinie tritt am Tage nach ihrer Bekanntmachung im Verkündungsblatt der Hochschule Hannover in Kraft.